

ШЫҒЫС № 326

АНЫҚТАМА

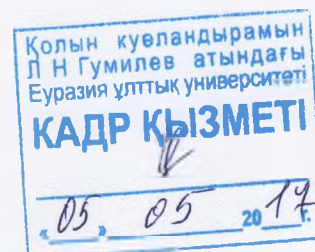
Осы анықтама Т.Хакимоваға, Л.Б. Рахимжановаға және Ж. Спабековаға «Ақпараттың қауіпсіздігін қалыптастырудағы сандық қол қою» атты мақалаларының «Л.Н.Гумилев атындағы ЕҰУ Хабаршысы» журналының 2017 жылғы 3 санына қабылданғандығын растау үшін беріліп отыр.

Әлеуметтік-мәдени даму
жөніндегі проректор

Типография бастығы

Д. Қамзабекұлы

Т.С. Жұманалин



Т.ХАКИМОВА¹, Л.Б. РАХИМЖАНОВА¹, Ж. СПАБЕКОВА²

*п.ғ.к., доцент, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ. ¹,
магистр, аға оқытушы, Әл-Фараби атындағы Қазақ ұлттық университеті
Алматы қ. ²,*

АҚПАРАТТЫҢ ҚАУІПСІЗДІГІН ҚАЛЫПТАСТЫРУДАҒЫ САНДЫҚ ҚОЛ ҚОЮ

Аңдатпа

Студенттердің жаңа технологияларды қолдануда, технологиялық жетістіктерге негізделген, криптография компьютерлік жүйелермен желілердегі ақпараттың қауіпсіздігін қамтамасыз ететін заманауи жүйелердің әдістемелік негізін пайдаланудың әдісі. Студенттерге осы ғылыммен, таныстыру және олардың ең қызықты аспектілерін олардың пайдасына оны тастай жабық құпиясын, пайдаланудың мүмкіндігі керек. Ақпараттық технологияларды мамандықтары бойынша оқытуда электрондық сандық қол қоюды үйрету білімді жоғарлатуға өте зор ықпал жасайды.

Түйінді сөздер: *оқыту, ақпараттық технологиялар, электрондық цифрлық қолтаңба, криптография.*

Қоғамда ақпараттандыру, есептеу техникасы құралдары кеңінен таралуымен байланысты, оқу процесін ұйымдастыруға, сол сияқты білім берудің мазмұнын өзгертуге де елеулі ықпал жасайды. Қазіргі заманғы оқыту интеллектуалдық ерекшеліктеріне сүйене отырып білім беруді жаңа инновацияларды пайдалануды қажет етеді. Білгір маман болып шығу үшін, ақпараттық технологияларды өте жетік меңгеру керек.

Осы жағдайда, қатынас құралдары кеңінен қолданысқа енгізілген уақытта, қауіпсіздік мәселесі өзекті мәселелердің біріне айналған. Криптография компьютерлік жүйелермен желілердегі ақпараттың қауіпсіздігін қамтамасыз ететін заманауи жүйелердің әдістемелік негізі болып табылады.

Студенттерге осы ғылыммен, таныстыру және олардың ең қызықты аспектілерін олардың пайдасына оны тастай жабық құпиясын, пайдаланудың мүмкіндігі керек. Компьютерлік техниканың көмегімен соңғы прогрессивті криптографияны пайдалануды қарастырып, электрондық сандық қолтаңбасының негізгі аспектілеріне қол жеткізу.

Тарихи тұрғыда криптография (грек тілінен аударғанда, бұл термин *құпия жазу* дегенді білдіреді) хабарламаларды жасырын жеткізу тәсілі ретінде туындаған. Криптография деректерді түрлендіру әдістерінің олардың құқысыз тұтынушыларға қажетсіз етіп, қорғауға бағытталған жиыны. Мұндай түрлендірулер деректерді қорғаудың біз атаған негізгі үш мәселесін – тасымалданатын немесе сақталатын деректердің құпиялылығын, біртұтастығын

және айқындығын қамтамасыз етуді – шешеді. Деректер қауіпсіздігін қамтамасыз ету үшін мынадай негізгі үш функция қолдануы қажет екенін айттық:

- тасымалданатын немесе жадта сақталатын деректердің құпиялығын қорғау;
- деректердің біртұтастығы мен айқындығын қолдау;
- абоненттер(тұтынушылар) жүйеге кіргенде және қосылғанда аутентификациялау.

Көрсетілген функцияларды жүзеге асыру үшін шифрлеудің сандық қол қоюдың және аутентификациялаудың криптографиялық технологиялары қолданылады.

(Криптология = криптография + криптоанализ)

Құпиялылық (конфиденциальный) шифрлеудің симметриялық және асимметриялық алгоритмдері мен тәсілдері көмегімен, сондай-ақ, абоненттерді көп қайталанатын және бір ретті парольдер, сандық сертификаттар, смарткарталар және т.б. өзара аутентификациялау арқылы қамтамасыз етіледі. Тасымалданатын деректердің тұтастығы мен айқындығына әдетте шифрлеудің біржақты функциялары мен асимметрияның тәсілдеріне негізделген электрондық қол қою технологияларының әртүрлі үлгілері көмегімен қол жеткізіледі.

Цифрлік қолтаңба деп кейбір құпиялы кілтті қолданумен генерацияланған блоктің мәліметтерін атайды. Бұнымен бірге, ашық кілт арқылы мәліметтердің сол құпиялы кілтпен генерацияланғанын тексеруге болады. Цифрлік қолтаңбаны генерациялау алгоритмі құпиялы кілтсіз тексеру кезінде дұрыс болатын қолтаңбаны жасауға жол бермеуін қамтамасыз етуі тиіс. Цифрлік қолтаңбалар хабардың шын мәнінде сол жіберушіден келгенін (тек хабарды жіберуші ғана оның ашық кілтіне сай құпиялы кілтті иеленгендіктен) растау үшін қолданылады. Сондай-ақ, қолтаңбалар уақыт мөртабанын қоюға (timestamp) қолданылады: сенім білдірілетін тарап өзінің құпиялы кілтімен уақыт мөртабанын қойып, құжатқа қол қояды және құжаттың мөртабан уақытында жарияланғанын растайды. Цифрлік қолтаңбаларды сонымен бірге, белгілі тұлғаға тиесілі екенін растауға куәлік үшін де қолдануға болады (сертификациялар — to certify). Ол мына жолмен іске асады: ашық кілт пен оның иесі туралы ақпаратқа сенім білдірілетін тарап қол қояды. Бұнымен бірге, сенім білдірілген тарапқа оның кілті үшінші тараптың қолы қойылғандықтан сенім артамыз. Әлдебір кілт иерархияның түпкі кілті болуы тиіс (оған әлдебіреудің қол қойылғандығынан ғана сенім білдірмейміз, біз a-priori сенеміз, оған сенім артуға болады дейміз). Кілттердің орталықтандырылған инфрақұрылымында желінің түпкі кілттерінің кішігірім саны ғана бар (мысалы, өкілеттігі бар мемлекеттік агенттіктер: оларды сондай-ақ, сертификацияланған агенттіктер деп атайды— certification authorities). Бөлінген инфрақұрылымда бәріне әмбебап түпкі кілттердің болудың қажеттілігі жоқ және де әр тарап өзінің түпкі кілттерінің жиынтығына ғана сене алады (айталық, өзінің жеке

кілті мен қолы қойылған кілттері). Бұл тұжырым сенім желісі деп аталады (web of trust) және де айталық, PGP-да іске асырылған. Тасымалданатын деректердің тұтастығы мен айқындығына әдетте шифрлеудің біржақты функциялары мен асимметрияның тәсілдеріне негізделген электрондық қол қою технологияларының әртүрлі үлгілері көмегімен қол жеткізіледі. Аутентификация тек әйгілі тұтынушылар арасындағы байланысқа рұқсат етіп, желінің құрал-жабдықтарына қажетсіз адамдардың қосылуына тосқауыл болады. Өздерінің мәртебесін дәлелдеген тұтынушыларға жүйелік қызметтің рұқсат етілген түрлері көрсетіледі [1].

Электрондық сандық қол қою телекоммуникация арналары арқылы тасымалданатын мәтіндерді аутентификациялау үшін қолданылады. Мұндай алмасу кезінде құжаттарды өңдеуге және сақтауға жұмсалатын шығындар едәуір төмендейді. Оларды іздеу жылдамдайды. Бірақ, электрондық құжаттың авторын және құжаттың өзін аутентификациялау, яғни автордың нақтылығын анықтау және қабылданған ЭҚ(электрондық құжаттың) құрамында өзгеріс жоқ екенін анықтау, мәселесі туындайды. ЭҚ аутентификациялаудың мақсаты төмендегі әр түрлі мүмкін зақымдау әрекеттерінен қорғау:

- Пәрменді (активный) бұрыпалу (перехват) – бұзушы желіге қосылып құжаттар мен файлдарды өзіне бұрып, оларды өзгертеді;
- Маскарад – абонент С абонент Б-ға абонент А-н атынан құжат жөнелтеді;
- Ренегаттық – абонент А өзі жөнелте отырып, абонент Б-ға ешқандай хабарлама жолдамағанын жолдайды;
- Алмастыру – абонент Б өзгертіп немесе жаңа құжат құрып оны абонент А-дан алдым деп жариялайды;
- Қайталау – абонент С абонент А-н абонент Б-ға жөнелткен құжатын қайталайды

Хабарламаның біртұтастығын және автордың нақтылығын тексеру мәселесін тиімді шешуге электрондық сандық қол қою әдістемесі мүмкіндік береді.

Сандық қол қоюдың негізгі процедуралары

Функционалдық түрде сандық қол қою әдеттегі қолмен қол қоюға ұқсас және оның негізгі артықшылықтарына ие:

- Қол қойылған мәтіннің қол қойған адамнан келетінін дәлелдейді;
- Қол қойған адамның қол қойылған мәтін мен байланысты міндеттерден бас тартуға мүмкіндік бермейді;
- Қол қойылған мәтіннің біртұтастығына кепілдік береді;

Электрондық сандық қол қою дегеніміз – қол қойылған мәтінмен бірге жіберілетін қосымша сандық ақпараттың салыстырмалы аз ғана жиыны. Электрондық сандық қол қою асимметриялық цифрлардың кері оқылатынына сондай-ақ хабарламаның мазмұнының қол қоюдың өзінің және кілттер жұбының өзара байланысқа негізделген. Аталған элементтердің біреуінің ғана өзгеруі сандық қол қоюдың нақтылығын анықтау мүмкіндігінен айырады. Электрондық сандық қол қою шифрлеудің асимметриялық алгоритмдері және ХЭШ функциялар көмегімен жүзеге асырылады. Электрондық сандық қол қою жүйесінің қолдану технологиясы бір-біріне қол қойылған электрондық

құжаттар жөнелтетін абоненттер желісі болуын болжайды. Әрбір абонент үшін кілттердің құпия және ашық жұптары қалыптастырылады. Құпия кілтті абонент жасырып Электрондық сандық қол қоюды қалыптастыру үшін пайдаланады. Ашық кілт басқа барлық тұтынушыларға да белгілі болып қол қойылған электрондық құжатты қабылдаушы Электрондық сандық қол қоюды тексеру үшін қолданылады[2]. Электрондық сандық қол қою жүйесі екі негізгі процедурадан тұрады:

- Сандық қол қоюды қалыптастыру;
- Сандық қол қоюды тексеру;

Қол қоюды қалыптастыру процедурасында хабарламаны жөнелтушінің құпия кілтті қолданылады, қол қоюды тексеру процедурасында жөнелтушінің ашық кілтті пайдаланылады.

Сандық қол қоюды қалыптастыру процедурасы.

Бұл процедураның дайындық кезеңінде абонент А – хабарламаны жөнелтуші – кілттер жұбын қалыптастырады: K_A құпия кілтін және K_A ашық кілтін. K_A ашық кілті оның жұбы K_A құпия кілтінен есептеледі. K_A ашық кілті желінің басқа абонентіне таратылады (немесе ортақ ресурста орналастырып басқалардың қол жеткізу үшін) қол қоюдың тексерген кезде қолданылады. Сандық қол қоюды қалыптастыру үшін жөнелтуші А ең алдымен қол қойылатын М мәтінінің $h(M)$ Хэш функциясының мәнін есептейді. Хэш функция бастапқы қол қойылатын М мәтіні m - дайджестіне – өзгермейтін аз ғана беттерден тұратын және М мәтінін тұтастай және жалпы сипаттайтын салыстырмалы қысқа сан сығу үшін қолданылады. Одан әрі жөнелтуші А М дайджестін өзінің құпия K_A кілтімен шифрлейді, осылай алынатын сандар жұбы осы М мәтіні үшін сандық қол қою болып табылады. М хабарламасы сандық қол қоюмен бірге қабылдаушының адресіне жөнелтіледі.

Сандық қол қоюдың тексеру процедурасы

Желінің абоненттері қабылданған М – хабарламаларының сандық қол қоюдың осы хабарламаны жөнелтушінің K_A ашық кілттің көмегімен тексере алады.

Электрондық сандық қол қоюды тексергенде абонент Б-М хабарламаларын қабылдаушы – қабылданған М дайджестін жөнелтуші А-н ашық K_A ашық кілтімен кері шифрлейді. Сонымен бірге қабылдаушының өзі $h(m)$ Хэш функцияларының көмегімен қабылданған М хабарламаларының m - дайджестін есептеп, оны кері шифрленген дайджестпен салыстырады. Егер m және m' тең болса онда сандық қол қою нақты және айқын болады. Кері жағдайда қол қою жасанды немесе хабарламаның мазмұны өзгертілген деп есептеледі. Электрондық сандық қол қою жүйесіндегі ең маңызды сәт тұтынушының электрондық сандық қол қоюдың оның қол қою үшін құрылған құпия кілтін білмей жасау мүмкін емес. Сондықтан рұқсат етілмеген қол жеткізулерден, қол қоюдың құпия кілтін сақтау қажет. Электрондық сандық қол қоюдың құпия кілтін симметриялық шифрлеудің кілтті сияқты жеке дара кілт тасымалдаушыда қорғалған түрде сақтау ұсынылады. Электрондық сандық қол қою дегеніміз – қол қойылатын құжаттан және абоненттің құпия кілтінен

тәуелді ерекше сан. Қол қойылатын құжат ретінде кез келген файлды алуға болады. Қол қойылған файл қол қойылмаған файлдан оған бір немесе бірнеше электрондық сандық қол қоюлар қосу (толықтыру жолмен) құрылады. Қол қойылатын файлға орналастыратын (немесе электрондық сандық қол қоюдың жеке файлына жазылатын) электрондық сандық қол қою құрамына әдетте қол қойылған құжаттың авторын бір мәнді анықтайтын (аутентификациялайтын) қосымша ақпарат кіреді. Бұл ақпарат құжатқа электрондық сандық қол қоюды есептегенге дейін қосылады, осы жолмен оның біртұтастығы қамтамасыз етіледі. Әрбір қол қою мынадай ақпараттан тұрады:

- Қол қою күні
- Осы қол қою кілтінің жарамды уақыты
- Файлға қол қойған адам туралы ақпарат (аты, тегі, әкесінің аты, қызметі, фирманың қысқаша аты)
- Қол қойған адамның идентификаторы (ашық кілттің аты)
- Сандық қол қоюдың өзі

Тұтынушы тұрғысынан сандық қол қоюды қалыптастыру және тексеру үдерісі тасымалданатын деректерді криптографиялық жасыру үдерісінен ерекшеліктері бар. Сандық қол қоюды қалыптастырғанда жөнелтушінің жабық кілті қолданылады, ал шифрлегенде қолданбалы ашық кілті қолданылады [3]. Сандық қол қоюды тексергенде жөнелтушінің ашық кілті қолданылады, деректерді кері шифрлегенде қабылдаушының жабық кілті қолданылады. Ақпаратты шифрлеу және кейін кері шифрлеу үшін әртүрлі кілттер қолданылады:

- *ашық кілті* ақпаратты шифрлеу үшін қолданылады
- *құпиялы кілті* оның жұбы болып табылатын ашық кілттің көмегімен шифрленген ақпаратты кері шифрлеу үшін қолданылады.

Ақпараттық технологияларды мамандықтары бойынша оқытуда электрондық сандық қол қоюды үйрету білімді жоғарлатуға өте зор ықпал жасайды.

Сонымен, біз электрондық қолтаңба туралы барлық білімімізді, оның түрлері, қолданудың негізгі салалары мен қыр-сырларын пайдалануға қостық. Бұл мақала ең алдымен электронды қолтаңбаның қыр-сырымен жұмысты түсінуге тиімді. Біз ең пайдалы, әрі қызықты теориялық мәліметтерді «жанадан бастаушы» жастар мен заманауи технологияларды белсенді қолданушыларға арнап жинақ жасауға тырыстық.

Пайдаланған әдебиеттер

- [1]. Шангин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «Форум»: ИНФРА-М, 2008.
- [2]. Петров А.А. Компьютерная безопасность: криптографические методы защиты. М.: ДМК Пресс, 2000.
- [3]. Хакимова Т. Мәліметтерді қорғауда шифрлаудің қарапайым әдістері.// Материалы международной научно-практической конференции «Актуальные

проблемы информатики и процессов управления». г. Алматы, 15-16 ноября 2012 года. Часть II. 406-411 стр.

References:

- [1]. Shangin V.F. Informatsionnaya bezopasnost' komp'yuternykh sistem i setey. – М.: ID «Forum»: INFRA-M, 2008.
- [2]. Petrov A.A. Komp'yuternaya bezopasnost': kriptograficheskiye metody zashchity. М.: DMK Press, 2000.
- [3]. Khakimova T. Mәlimetterdi k,orgauda shifrlaudıñ k,arapayym әдіsteri .// Materialy mezhdunarodnoy nauchno-prakticheskoy konferentsii «Aktual'nyye problemy informatiki i protsessov upravleniya» .g.Almaty, 15-16 noyabrya 2012 goda. Chast' II. 406-411 str.

ЦИФРОВАЯ ПОДПИСЬ ПРИ ФОРМИРОВАНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В статье рассматриваются основные методы применения студентами технологических достижений современной криптографии для обеспечения безопасности компьютерных систем, сетей, информационных систем. Студентов знакомят с тайнами с этой науки, с ее наиболее интересными аспектами, чтобы они могли использовать ее возможности себе на пользу. Обучение электронной цифровой подписи будет способствовать значительному увеличению знаний в области информационных технологий.

Ключевые слова: обучение, информационные технологии, электронная цифровая подпись, криптография.

DIGITAL SIGNATURE IN THE FORMATION OF INFORMATION SECURITY

Abstract

The article deals with the basic methods of use of students of the technological advances of modern cryptography to ensure the security of computer systems, networks and information systems. Students are introduced to the secrets of this science, with its most interesting aspects, so that they can use this opportunity to their advantage. Education digital signatures will facilitate a significant increase in information technology knowledge.

Keywords: training, information technology, digital signature, cryptography.

Хакимова Тиыштық

Хакимова Тиыштық

Tiyshtik Khakimova

Рахимжанова Ләззат Балтабайқызы

Рахимжанова Ляззат Болтабаевна

Rakhimzhanova Lyazzat

Спабекова Жанар

Spabekova Zhanar