УДК 372.851.02УДК 372.800.4.02

Т.Х. Хәкімова

Әл-Фараби атындағы Казақ ұлттық университеті, Алматы,Казахстан

ЭЛЕКТРОНДЫҚ САНДЫҚ ҚОЛ ҚОЮ ТЕХНОЛОГИЯСЫНЫҢ АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАРДЫ ОҚЫТУДАҒЫ РӨЛІ

резюме

О роли использованя технологии электронной цифровой подписи в обучении Информационных технологии для професиональных целей студентов.

Summary

On the role of using digital signature technology in information technology training for students of Professional goals.

Қоғамда ақпараттандыру, есептеу техникасы құралдары кеңінен таралуымен байланысты, оқу процесін ұйымдастыруға, сол сияқты білім берудің мазмұнын өзгертуге де елеулі ықпал жасайды. Қазіргі заманғы оқыту интелектуалдық ерекшеліктеріне сүйене отырып білім беруді жаңа инновацияларды пайдалануды кажет 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 қаматамасыз ететін заманауи жүйелердің әдістемелік негізгі болып табылады. 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 тұрлендірулер 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 (конфидициальный) 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.

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-ң 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-ң 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

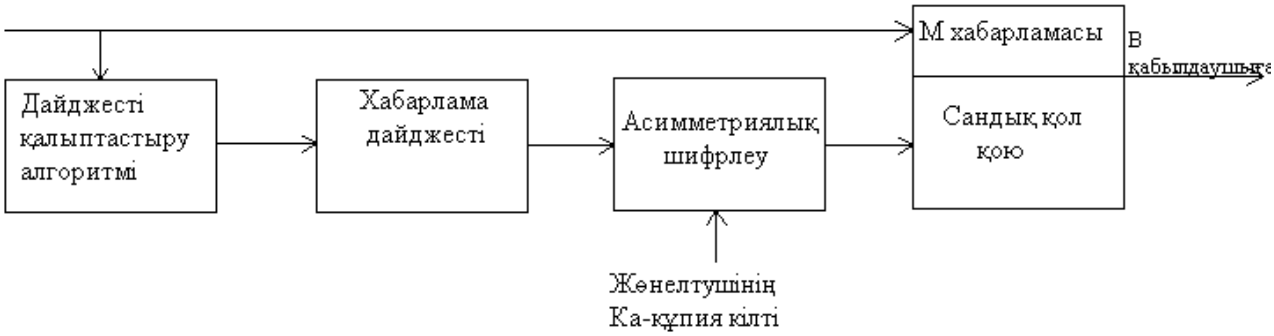
жиыны. Электрондық сандық қол қою асимметриялық цифрлардың кері оқылатынына сондай-ақ хабарламаның мазмұнының қол қоюдың өзінің және кілттер жұбының өзара байланысқа негізделген. Аталған элементтердің біреуінің ғана өзгеруі сандық қол қоюдың нақтылығын анықтау мүмкіндігінен айырады. Электрондық сандық қол қою шифрлеудің асимметриалық 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. Электрондық сандық қол қою жүйесі екі негізгі процедурадан тұрады:

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

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

Сандық қол қоюды қалыптастыру процедурасы.

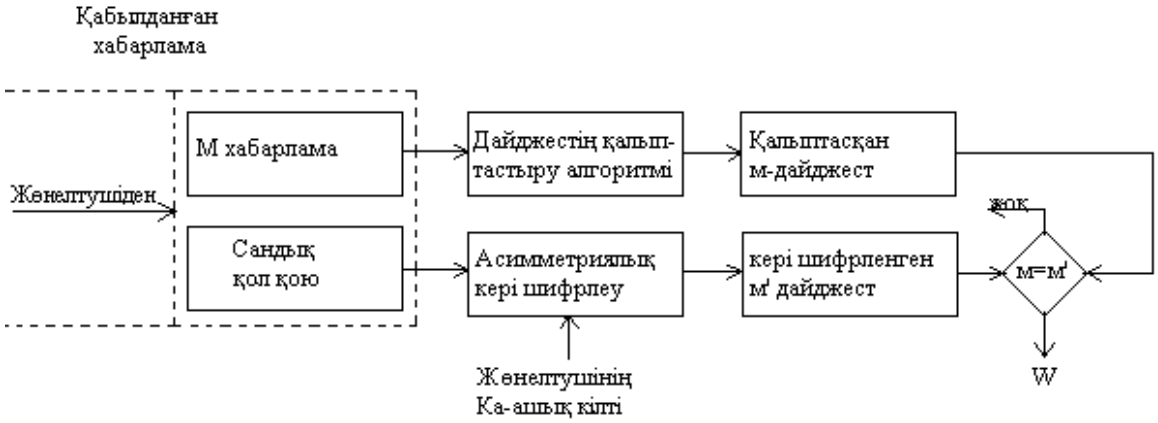
Бұл процедураның дайындық кезеңінде абонент А – хабарламаны жөнелтуші – кілттер жұбын қалыптастырады: $К_А$ құпия кілтін және $К_А$ ашық кілтін. $К_А$ ашық кілті оның жұбы $К_А$ құпия кілтінен есептеледі. $К_А$ ашық кілті желінің басқа абонентіне таратылады (немесе ортақ ресурста орналастырып басқалардың 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 м- 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 $К_А$ кілтімен шифрлейді, осылай алынатын сандар жұбы осы М мәтіні үшін сандық қол қою болып табылады. М хабарламасы сандық қол қоюмен бірге қабылдаушының адресіне жөнелтіледі.



Электрондық сандық қол қоюды қалыптастыру тәсілі

Сандық қол қоюдың тексеру процедурасы

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



Электрондық сандық қол қоюды тексеру тәсілі

Электрондық сандық қол қоюды тексергенде абонент Б-М хабарламаларын қабылдаушы – қабылданған М дайджестін жөнелтуші А-ң ашық $К_А$ ашық кілтімен кері шифрлейді. Сонымен бірге қабылдаушының өзі h(м) Хэш функцияларының көмегімен қабылданған М хабарламаларының м- дайджестін есептеп, оны кері шифрленген дайджестпен салыстырады. Егер м және м’ 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 кілті 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 мынадай ерекшеліктері бар . Сандық қол қоюды қалыптастырғанда жөнелтушінің жабық кілті қолданылады, ал шифрлегенде қолданбалы ашық кілті қолданылады. 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.

Әл-Фараби атындағы Казақ ұлттық университетінің барлық факультеттерінде «Ақпараттық технологияларды мамандықтары бойынша» оқыту пәні жүреді.Бекітілген Силлабустағы тақрыптарға сәйкес зертханалық сабақтарда, мысалдар қарастырылады;

1. «КОМПЬЮТЕРНЫЙ КЛАСС» хабарламаға киптоталдау жүргізу, Цезар шифрын қолдану арқылы.

Тақырыбы: Көпалфавитті шифр. Плейфейр шифры.

Мақсаты - дешифрлеу, Плейфейр матрицасы, символдарды қайта қою, ауыстыру шифры әдісі.

Плейфейр шифрының негізі хабарлама кез-келген ретпен орналасқан әріптерден тұратын кестеден шифрланып алынады Оның негізгі қадамдары:

1 қадам. Хабарлама екі әріпке (биграммаларға) бөлінеді. Мәтін көлемі жұп саннан тұрады, онда биграмма бірдей әріптерден тұрмауы қажет.

2 қадам. Егер биграмма бір бағанда, қатарда тұрмаса биграмманың екінші әріпін төртбұрыштың қарсы бұрышынан іздейді.

3 қадам. Егер биграмманың екі әріпі кестенің бағанында орналасса, онда одан төменгі әріп алынады. Егер биграмма төменгі жақта болса, сол қатардың басындағы бірінші әріп алынады.

4 қадам. Егер биграмма кестенің қатарында орналасса, биграмма әріпінің оң жағындағы әріпі алынады. Егер әріп қатардың соңында орналасса, онда сол қатардың бірінші әріпін алады.

Студентке берілген тапсырма: Биграммаларға бөлу, шифрлеу, дешифрлеу.

1. Ақпарат
2. Механика-математика
3. Убпоргвл-пбудпбфжвл
4. Әл – Фараби
5. Лето, зима

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

Пайдаланған әдебиеттер

1. Хакимова Т.Х.. Мәліметтерді қорғауда шифрлаудің қарапайым әдістері. // Материалы международной научно-практической конференции«Актуальные проблемы информатики и процессов управления».г.Алматы, 15-16 ноября 2012 г. Часть II.406-411стр.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах.-М.: Издательский центр «Академия», 2006г.