№14 Лекция тақырыбы: Электронды цифрлы қолтаңба технологиясы. Құжаттарды аутентификациялау.

Лекцияның оқыту нәтижелері: Электронды цифрлы қолтаңба (ЭЦҚ) ұғымын, оның мәнін және атқаратын қызметін түсіндіреді; ЭЦҚ-ның криптографиялық негіздерін, құрылымын және қолдану салаларын сипаттай және ЭЦҚ алу, пайдалану және тексеру алгоритмдерін тәжірибе жүзінде қолдана біледі.

Лекция мазмұны:

Электронды цифрлы қолтаңбаны қолдану технологиясы

Электронды цифрлы қолтаңбаны (ЭЦҚ) іске асыру алгоритмдерінде қолданылатын математикалық сызбалар біржақты функцияларда негізделген.

Бұл біржақты функцияларды қолдану келесі мәселелерге негізделген: әрбір жіберуші (жүйенің қолданушысы) алушыға (басқа қолданушыға) *x* құжаттағы өзінің *E(x)* ЭЦҚ-сын тексеру үшін қолданатын *E* процедурасын беруі керек немесе жалпыланған электрондық поштаға салып қою қажет. Өзінің ЭЦҚ-сын қоятын түпнұсқа жүйесін *D* жіберуші құпияда ұстауы қажет.

ЭЦҚ жүйесінде *x* құжаты орнына арнайы қасиеттер тізіміне ие болатын, солардың ішінен ең маңыздысы «коллизий» (яғни, хэш- функциясының мәні бірдей болатын, екі өзге құжатты жасауға тәжірибелік мүмкіндік жоқтығы) болдырмайтын оның хэш- функциясын қолданады *H(x)*. ЭЦҚ-ның ең белгілі математикалық схемалары: RSA, OSS (H. Ong, C. P. Schnorr, A. Shamir), Эль-Гамаля, Рабина (M. Rabin), Окамото (T. Okamoto), DSA (Digital Signature Algorithm), Мацумото-Имаи (T. Matsumoto, H. Imai), Микали-Шамир (Mikali, A. Shamir).

Бұл сызбаларындағы ЭЦҚ-ның күрделігі факторизациялау немесе дискретті логарифмдеу есебін есептеуге негізделген. Ұсынылған алгоритмдер ішінен А. А. Грушо (1992 ж.) айрықша сызбасын атап өтуге болады. Оның біржақты функциясының ерекшелігі, жоғарыда айтылғандай теоретикалық-сандық есептің қиындығында емес, ал оның күрделілігі сызықтық емес бульдік теңдеулер жүйесін шешу қиындығында. АҚШ және Ресейде ЭЦҚ-ға (DSS-Digital Signature Standard, ГОСТ 34. 10-94 және Р34.11-94) қабылданған стандарттарда арнайы жасалған алгоритмдер қолданылады. Бұл алгоритмдер Эль- Гамаль және Шнорр дербес алгоритмдеріне негізделген.

ЭЦҚ жүйесін қолдану технологиясы бір-біріне электронды құжаттар жіберетін қолданушылар желісін қарастырады. Бұл қолданушылар, басқалар қолтаңба қойған хабарламаларды тек тексере алады, ал енді бір қолданушылар (оларды қолтаңба қоюға құқығы бар қолданушылар деп атаймыз) қолтаңбаны тексере алады және қолтаңба қоя да алады. Бұл жадайда қолтаңбаны тексере алатын және қолтаңба қоя да алатын, мысалы, директор және бухгалтер болуы мүмкін.

Әрі қарай екі жағдай болуы мүмкін: бұл желіде орталығы бар (айрықша өкілеті бар ерекшеленген қолданушы) немесе барлық қолданушылар қолтаңба құқығымен бірдей. Сонымен бірге орталықтың жұмыстарының бірнеше локальды орталықтарға таратылған варианты да болуы мүмкін. Орталығы бар желілер қолданушылардың орталыққа деген сенімділігінің дәрежесі бойынша классификациялануы мүмкін. Мұндай желілердегі орталықтар қолданушыны толық бақылауы мүмкін немесе желіге жаңа қолданушыларды енгізу сияқты әкімшіліктің тек формалды функцияларын атқаруы мүмкін.

1.Электронды цифрлы қолтаңбаны қолдану технологиясы

Электронды цифрлы қолтаңбаны (ЭЦҚ) іске асыру алгоритмдерінде қолданылатын математикалық сызбалар біржақты функцияларда негізделген.

Бұл біржақты функцияларды қолдану келесі мәселелерге негізделген: әрбір жіберуші (жүйенің қолданушысы) алушыға (басқа қолданушыға) *x* құжаттағы өзінің *E(x)* ЭЦҚ-сын тексеру үшін қолданатын *E* процедурасын беруі керек немесе жалпыланған электрондық поштаға салып қою қажет. Өзінің ЭЦҚ-сын қоятын түпнұсқа жүйесін *D* жіберуші құпияда ұстауы қажет.

ЭЦҚ жүйесінде *x* құжаты орнына арнайы қасиеттер тізіміне ие болатын, солардың ішінен ең маңыздысы «коллизий» (яғни, хэш- функциясының мәні бірдей болатын, екі өзге құжатты жасауға тәжірибелік мүмкіндік жоқтығы) болдырмайтын оның хэш- функциясын қолданады *H(x)*. ЭЦҚ-ның ең белгілі математикалық схемалары: RSA, OSS (H. Ong, C. P. Schnorr, A. Shamir), Эль-Гамаля, Рабина (M. Rabin), Окамото (T. Okamoto), DSA (Digital Signature Algorithm), Мацумото-Имаи (T. Matsumoto, H. Imai), Микали-Шамир (Mikali, A. Shamir).

Бұл сызбаларындағы ЭЦҚ-ның күрделігі факторизациялау немесе дискретті логарифмдеу есебін есептеуге негізделген. Ұсынылған алгоритмдер ішінен А. А. Грушо (1992 ж.) айрықша сызбасын атап өтуге болады. Оның біржақты функциясының ерекшелігі, жоғарыда айтылғандай теоретикалық-сандық есептің қиындығында емес, ал оның күрделілігі сызықтық емес бульдік теңдеулер жүйесін шешу қиындығында. АҚШ және Ресейде ЭЦҚ-ға (DSS-Digital Signature Standard, ГОСТ 34. 10-94 және Р34.11-94) қабылданған стандарттарда арнайы жасалған алгоритмдер қолданылады. Бұл алгоритмдер Эль- Гамаль және Шнорр дербес алгоритмдеріне негізделген.

ЭЦҚ жүйесін қолдану технологиясы бір-біріне электронды құжаттар жіберетін қолданушылар желісін қарастырады. Бұл қолданушылар, басқалар қолтаңба қойған хабарламаларды тек тексере алады, ал енді бір қолданушылар (оларды қолтаңба қоюға құқығы бар қолданушылар деп атаймыз) қолтаңбаны тексере алады және қолтаңба қоя да алады. Бұл жадайда қолтаңбаны тексере алатын және қолтаңба қоя да алатын, мысалы, директор және бухгалтер болуы мүмкін.

Әрі қарай екі жағдай болуы мүмкін: бұл желіде орталығы бар (айрықша өкілеті бар ерекшеленген қолданушы) немесе барлық қолданушылар қолтаңба құқығымен бірдей. Сонымен бірге орталықтың жұмыстарының бірнеше локальды орталықтарға таратылған варианты да болуы мүмкін. Орталығы бар желілер қолданушылардың орталыққа деген сенімділігінің дәрежесі бойынша классификациялануы мүмкін. Мұндай желілердегі орталықтар қолданушыны толық бақылауы мүмкін немесе желіге жаңа қолданушыларды енгізу сияқты әкімшіліктің тек формалды функцияларын атқаруы мүмкін.

2.Құжаттарды аутентификациялау

Қағазсыз информатика байланыс желілері немесе машиналық тасымалдауыштар арқылы құжаттармен (бұйрықтармен, хаттармен және т.с.с.) айырбас жасау кезінде көптеген артықшылықтар береді. Бұл жағдайда уақытша шығындар (құжатты баспаға шығару, қайта жіберу, алынған құжатты клавиатурадан енгізу) көп азаяды, құжаттарды іздеу жылдамдайды, оларды сақтау шығындары азаяды және т.с.с. Бірақ бұл кезде құжаттың авторын және құжаттың өзін аутентификациялау қиындығы пайда болады (яғни, қолтаңбаның ақиқаттығын және алынған құжатта өзгеріс жоқ екендігін анықтау). Бұл қиындықтар кәдімгі (қағаздық) информатикада құжаттағы ақпарат жеке тұлғамен (қағазбен) тығыз байланысты болғандықтан оңай шешіледі. Машиналық тасымалдағыштарда мұндай байланыс жоқ.

Аутентификациялау қиындығы есептегіш желілерде, электронды басқару жүйелерінде және жалпы, байланыс арналары немесе машиналық тасымалдауыштар арқылы алынған хабарламаның (құжаттың) ақиқаттығын анықтау керек болатын жерлерде маңызды болып келеді.

Аутентификациялау мәселелерін келесі түрлерге бөлуге болады: қолданушыны аутентификациялау, қолданушының берілген топқа сай екендігін аутентификациялау, машиналық тасымалдауыштарда сақтаулы құжаттарды аутентификациялау.

Ең маңыздысы ретінде құжаттарды (немесе файлдарды) аутентификациялауға тоқтаймыз. Егер құпия құжаттармен айырбас жасау жағдайы қарастырылса (әскери немесе дипломатиялық байланыс), онда айырбас жасау сенімді және сенімге сай жақтар арасында жүзеге асырылатындығын жоғары дәрежелі сенімділікпен қарауға болады. Бірақ айырбас жасау, қиын есептеулер жүргізе алатын қарсыластың бақылауында және басқаруында болуы мүмкін, кейіннен ол өзінің құжаттарын жасауы немесе заңды жіберушінің құжатын ұстап алып, оны өзгертуі мүмкін. Басқа сөзбен айтқанда, бұл тек қарсыластан қорғану керек жағдай – «өзіміздікі» алдай алмайды.

Коммерциялық әлемде бұл жағдай керісінше болуы мүмкін, яғни жіберуші мен алушы «өздерінікі» болғанымен, басқаларға қарағанда бір-бірін көп дәрежеде алдауы да мүмкін.

Бірінші жағдайда («өздерінікі алдамайды») аутентификациялау сызбасын құру қиын емес. Жіберуші мен алушы қолданушыларды сенімді шифрмен және әрбір жіберілетін құжат үшін қолайлы кілттер жабдықтау арқылы қорғалған байланыс арнасын қамтамасыз етеміз. Қарастырылып отырған мәселе шифрлау жүйесіне жоғары талаптар қоятынын айтып кетейік. Айталық гаммирлеу әдісі бұл жағдайда қолдануға келмейді, себебі қарсылас ашық және жабық мәтінді сораптап гамманы алады да, кез келген өзіне керек мәтінді тіркеп жібере алады. Алайда, қойылған талаптарды қанағаттандыратын жылдам шифрлау алгоритмдері бар.

Екінші жағдайда («қолданушылардың кез келгені алдауы мүмкін болғанда») классикалық криптографияға негізделген әдісті қолдана алмаймыз, себебі құпиялы кілті бар қарсыластың зиянды әрекеттер жасауына толық мүмкіндігі бар. Мысалы, құжатты алушы жақ кез келген құжатты генерациялап өзіндегі алушыға да, жіберушіге де ортақ кілтпен шифрлап, содан соң, ол құжатты заңды жіберушіден алдым деуі мүмкін. Бұл жерде екі кілтті криптографияда негізделген сызбаны қолдану керек. Бұл жағдайда жіберушіде өзінің құпиялы кілті болады, ал алушыда жіберушінің құпиялы емес ашық кілті болады. Бұл ашық кілтпен жіберушінің қолтаңбасының ақиқаттығын тексеруге болады да, ол арқылы құпиялы кілтті шығарып алуға болмайды. Жіберуші өзінің жабық кілтіне жеке жауапкершілік білдіреді. Өзінен басқа ешкім қолтаңба генерациялай алмайды. Құпиялы кілтті жіберушінің жеке мөрі ретінде қарастыруға болады, сондықтан кілттің иесі оған басқа бөгде адамдардың қол жеткізуін шектеуі қажет.

Аутентификациялаудың жалпыланған моделі болып төрт қатысушылар түрі қарастырылады (7-сурет): *A* жіберуші, *B* алушы, *C* қарсылас(қаскүнем) және *D* арбитр. Бұл жағдайда *A* хабарлама жібереді, *B* алушы, *C* қарсылас әрекет жасағысы келеді, ал *D* даулы жағдайларда шешім қабылдайды, яғни қай жақтан қателік кеткенін анықтайды. Әрине, *C* ретінде *A* және *B* болуы мүмкін.

7-сурет. *Ақпараттық айырбас және қауіп төндіру моделі*

Құжаттарды аутентификациялаудың негізгі мақсаты әртүрлі мүмкін қарсылас әрекеттерден қорғау, солардың ішінен бөліп көрсетейік:

1. *Активті ұстап алу* –қарсылас желіге жалғанып алып құжаттарды (файлдарды) ұстап алады және оларды өзгертеді;

2. *Маскарад – C* құжатты *A-ның* атынан жібереді;

3. *Ренегаттылық – A* хабарламаны *B*-ға жібергенімен жіберген

жоқпын деп мәлімдейді;

4. *Өзгерту – B* құжатты өзгертеді де, сол құжатты (өзгертілген) *A*-дан алдым деп мәлімдейді;

5. *Ауыстыру – B* құжат (жаңа) жасайды да, оны *A*-дан алдым деп мәлімдейді;

6. *Қайталау-A*-ның *B*-ға бұрын жіберген құжатын *C*-ға қайталап жібереді.

Бұл қарсылас әрекеттердің түрлері, өз қызметінде компьютерлік ақпараттық технологиялар қолданатын банктердің, коммерциялық құрылымдардың, мемлекеттік кәсіпорындардың және ұйымдардың, жеке тұлғалардың жұмыстарына маңызды зияндарын тигізеді. Сондықтан қарсылас әрекеттер жасау мүмкіншілігі, компьютерлік технологияларға сенімділікті кеміте түсіреді. Осыған байланысты аутентификациялау мәселесі маңызды болып келеді.

Желідегі хабарламаларды аутентификациялау алгоритмі мен технологияларын таңдаған кезде, жоғарыда көрсетілген қарсылас әрекеттердің барлық түрлерінен қорғайтындай етіп алу керек. Аутентификациялау жүйесінің мұндай қасиеттерімен бірге оның жылдамдығы және іске асыру үшін керек жады көлемі, жоғарыда көрсетілген қауіптерден қорғау дәрежесі (беріктілігі) маңызды болып табылады.

Оқытудың техникалық құралдары: Компьютер, ноутбук, интернет.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру және мысалдар арқылы көрсету
- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау
- Қорытынды сұрақтар мен талқылау

Оқыту әдістері мен түрлері:

- Түсіндірмелі-баяндамалық әдіс
- Көрнекілік және демонстрациялық әдіс
- Практикалық тапсырмалар орындау
- Интерактивті сұрақ-жауап және топтық талқылау

БӨЖ және ОБӨЖ тапсырмалары,олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

БӨЖ: RSA криптожүйесі арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллды құрайды.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -20 балл
- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: RSA криптожүйесі арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллды құрайды.

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- **БӨЖ — 60% (60 балл)**
- **ОБӨЖ — 40% (40 балл)**

Пайдалынатын әдебиеттер тізімі:

Негізгі:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Кауфман Ч., Перлман Р., Спеснер М. *Network Security: Private Communication in a Public World.* – Prentice Hall, 2016.

3. Schneier B. *Applied Cryptography.* – Wiley, 2015.

4. Stallings W. *Cryptography and Network Security: Principles and Practice.* – Pearson, 2022.Таненбаум Э. Компьютерлік желілер. – Алматы: Эверо, 2019

5. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

Қосымша:

1. Ахметова, С. Бағдарламалау технологиясы : Лекция жинағы. / ЮКГУ им. М.О. Ауезова. - Шымкент: ОҚМУ, 2007. - 51 б. https://rmebrk.kz/book/50006

2. Ж.З. Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтурсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz