Институт информационных и
вычислительных технологий
МОН РК

МАТЕРИАЛЫ

научной конференции
Института информационных и
вычислительных технологий
МОН РК
«Современные проблемы информатики
и
вычислительных технологий»
2 - 5 июля 2018 года

IICT

Алматы 2018

дін иелері. Өз дәрежесіне сәйкес, мәселен, тәре 15-16, ал қожа 7-8 нөкерін ер
жүретін болған...

Көне есептердің осындай сипаттарын көптеп келтіруге болады және олар
анықтап бір жүйеге түсіріп, олардың ауыз әдебиетінде алатын орнын анықтау – бүгін
ғылым алдына қойылар басты міндетінің бірі деп есептейміз. Бұндай мәселе
гуманитарлық және нақты ғылымдар арасындағы пәнаралық байланыс, жалғастық пе
сабақтастықтың арқасында орындалмақ. Атап айтқанда, көптеген байырғы көн
есептер халық тұрмысындағы болар жағдайды пайымдау, істелмек нәрсені алдын ал
мейлінше ұқыптылықпен бағдарлау және оларды нақты есептей отыра жобалау
олардың тиімділігіне алдын ала көз жеткізу мақсатында өмірге келген. Демек, осы
жағдайға тиянақты зер салсақ, ғылымның пән аралық байланыс тәсілі осы аталып
отырған ғылыми мәселені тиянақты атқаруға толықтай мүмкіндік береді.

Есептеу ғылымы қалыптаспаған ортада есеп үлгілерінің болуы мүмкін еместігі
баршамызға мәлім. Ендеше, байырғы көне есептер тек қана дәстүрлі ортада, яғни
логикалық ойлау қабілеті жоғары дамып, есеп құрастыру және оны ауызша шығару
дәстүрі орныққан және де шығармашылық қабілеті ерекше өркендеп, есте сақтау
қабілеті кемелденген ортада ғана пайда болып дами алатыны түсінікті құбылыс.
Демек, байырғы Ұлы Дала есептері ерте заманның өзінде-ақ қазақ халқының
логикалық ойлау жүйісі мен шығармашылық қабылеттері ерекше дамыған ел
болғанын көрсететін қасиетті тарихи құндылық және рухани мұра.

Егер байырға қазақи көне есептер ұрпақтан ұрпаққа, ғасырдан ғасырға қағаз
бетіне түсірілмей-ақ халық жадында сақталып келе жатқанын еске алсақ, онда олар
халық ауыз әдебиетінің ерекше танымдық нысаны екені түсінікті болады. Олардың
мыңдаған жылдар бойы халық жадында мәңгілік орын алған рухани құндылық екені
айқындала түседі.

Міне осындай себептермен Президент Н.Назарбаев ***«Болашаққа бағдар: рухани жаңғыру»*** атты өзекті мақаласында: «*...Ұлттық жаңғыру дегеннің өзі ұлттық сананың кемелденуін білдіреді. Оның екі қыры бар. Біріншіден, ұлттық сана-сезімнің көкжиегін кеңейту. Екіншіден, ...құндылықтар жүйесінде білімді бәрінен биік қоятын ұлт қана табысқа жетеді*» деп жазды.

Ендеше, еліміздің әрбір азаматы үшін ұлттық сана-сезімнің көкжиегін кеңейтуге, қасиетті ұлттық рухани құндылықтың кемелденуіне бір адамдай атсалысу үлкен де ұлағатты абзал борыш.

Бұл мақала Қазақстан Республикасы Оқу және Білім министрлігі Білім комитетінің «Мәңгілік Ел» ғылыми негіздері» атты ғылымды дамытудың басым бағытының Бағдарламалық-нысаналы қаржыландыру шеңберінде №BR05236075 «***Ұлы Даланың байырғы көне есептерін қазақ халқының қасиетті рухани мұрасы және фольклорлық құндылығы ретінде зерттеу, талдау және жаңа жүйеге келтіру***» атты ғылыми-техникалық бағдарлама бойынша жазылды.

КРИПТОГРАФИЯЛЫҚ ЖҮЙЕЛЕРДЕ КІЛТТЕРДІ БАСҚАРУ

Капалова Н., Хаумен А., Абишева А.

ҚР Білім және ғылым министрлігі Ғылым комитетінің «Ақпараттық және есептеуіш технологиялар институты», Қазақстан
e-mail: *kapalova@ipic.kz, haumen.armanbek@gmail.com, ak_maral@mail.ru*

Аннотация. *Бұл мақалада позициялық емес полиномдық санау жүйелерінің негізінде құрылған ақпаратты криптографиялық қорғау алгоритмдеріндегі кілтерді басқару сұрақтары қарастырылған. Криптографиялық кілттерді генерациялау, жинақтау және тарату мәселелері талқыланып, оларды шешудің жолдары, құрылымы мен қасиеттеріне шолу жасалынады. Сонымен қатар позициялық емес полиномдық санау жүйелеріне негізделіп құрылған алгоритмнің кілттік құрылымы да қарастырылады.*

Ақпараттық қауіпсіздікті қамтамасыз ету – ақпараттық технологияларды дамытудың басым бағыттарының бірі. Осы салада шешілген мәселелердің ауқымы сандық және сапалық тұрғыда үнемі кеңеюде. Компьютерлік жүйелерде ақпаратты қорғау үшін қолданылатын негізгі құралдардың бірі криптографиялық түрлендірулер болып табылады. Заманауи криптографияның төрт басты бөлімі бар: симметриялы криптожүйелер, ашық кілтті жүйелері, электронды қолтаңба жүйесі, кілттерді басқару.

Қазіргі уақытта криптожүйелер кілттерді пайдалануға негізделген. Кілттерді басқару ақпарат алмасудың құпиялығын, деректердің сәйкестілігін және тұтастығын қамтамасыз ету үшін шешуші рөл атқарады. Әдетте, кілттерді басқару криптографиялық қосымшалардың ең осал тұсы болып табылады. Криптографиялық технологияны пайдалану қарапайым, бірақ кілттерді сақтау, кілттерді пайдалану және олардың өзара алмасуын қамтамасыз ету әлдеқайда қиын болып табылады. Сенімділігі төмен кілттік басқару жүйесі өте жақсы ұйымдастырылған жүйелердің сапасын төмендетеді, өйткені алгоритмнің бар қауіпсіздігі кілттердің қауіпсіздігіне шоғырланған.

Алайда заманауи криптографияның алдында тұрған негізгі мәселелер, бұл алгоритмнің тұрақтылығын арттыру және кілттер мен мәліметтер блогының мөлшерін азайту. Бұл мәселені шешудің ең айқын жолы-криптографиялық алгоритмдердегі ақпараттар блогын тек сандар түрінде (немесе ақырлы өрістің элементтерін) көрмей, оларды басқа да үлкен қиындықты алгебралық обьект түрінде көру. Осындай типтегі объектілер қатарына позициялық емес полиномды санау жүйелері (ПЕПСЖ) жатады [1-3].

Ақпараттық және есептеуіш технологиялар институтының ақпараттық қауіпсіздік зертханасында позициялық емес санау жүйелеріне негізделген ақпаратты шифрлеу алгоритмдері құрастырылып, сынақтан өтуде [4]. Практикалық іске асыру және теориялық зерттеулер нәтижелері көрсеткендей, осы ПЕПСЖ-сін дәстүрлі емес алгоритмдер мен кодтау әдістерін құрастыруда және шифрлауда, электрондық сандық қолтаңбаны (ЭСҚ) қалыптастыруда пайдалану, осы криптографиялық рәсімдердің айтарлықтай сенімділігін арттыруға, ЭСҚ-ның ұзындығын азайтуға мүмкіндік береді. Ұсынылған алгоритмдер криптографиялық тұрғыда жақсы қасиеттерге ие екені арнайы жүргізілген сынақтардың қорытындысы дәлелеледеп берді [5]. Ендігі кезекте осы шифрлеу алгоритмдеріне негізделген крипторгафиялық жүйеге қажетті кілттерді басқару мәселесі туындап отыр.

Кілттерді басқару процедурасына **кілттерді жасау, оларды жинақтау және тарату** қызметтері жатады [6]. Осыларға шолу жасап, міндеттері мен функцияларын сипаттап өтейік. Жақсы ұйымдастырылған кілттерді басқару жүйесінің маңызды сипаты бірнеше кілттердің қауіпсіздігін қамтамасыз ету мәселесіне көптеген кілттердің қауіпсіздігін қамтамасыз етудің күрделі мәселелерін біріктіру болып табылады. Сақталатын ақпараттың қауіпсіздігін қамтамасыз ету үшін кілттерді қолданған жағдайда, субъекті бір пайдаланушы болуы мүмкін және ол дәйекті уақыт

аралығында деректермен жұмыс істейді. Байланыс желілеріндегі кілттерді басқару ке
дегенде екі субъектіні қамтиды – хабарды жіберуші және алушы.

Негізгі кілттерді басқарудың мақсаты – қауіптерді бейтараптандыру. О
қауіптерге мыналарды жатқызуға болады:

- Жеке кілттердің құпиялылығын бұзу;
- Ашық немесе жабық кілттердің шынайылығын және аутентификациялығы
бұзу. Бұл жерде шынайылық ретінде осы кілтті қолданатын желіні
конфиденциалдығын қамтамасыз ету үшін корреспонденттің түпнұсқалылығын біл
немесе тексеру мүмкіндігін түсінеміз;
- Ашық немесе жабық кілттерді рұқсатсыз пайдалану, мысалы, кілтті пайдалану
мерзімі аяқталған кезде.

Кілттерді басқару функциялары мыналарды қамтиды:

- ЭЦҚ кілттерін қалыптастыру;
- Ашық кілтті тіркеу және тіркеу туралы куәлікті беру;
- Ашық кілтті куәліктің қолданылу мерзімін белгілеу;
- Ашық кілттерге қол жеткізуді ұйымдастыру;
- Сертификат мәртебесін анықтау;
- Қайтарып алудың себебін көрсететін куәліктерді қайтарып алу;
- Сертификаты тоқтата тұру / ұзарту;
- Сертификаттарды мұрағаттау;
- Сертификаты және қауіпсіздік саясатын пайдалануды басқару [7].

Кілттерді **жасаудың** қолданыстағы әдістерін аппараттық және бағдарламалық деп бөлуге болады. Бұл жағдайда басты талап – кілттердің үлестірімінің бірқалыптылығы. Кілттерді аппараттық жасау кезінде кездейсоқ физикалық процесс жүретін электрондық құрылғылар – шу генераторлары қолданылады.

Бағдарламалық іске асыруда - псевдокездейсоқ тізбек генераторлары қолданылады. Псевдокездейсоқ сандық генераторларды таңдағанда арнайы критерийлер орындалуы қажет [8].

Кілттерді **жинақтауды** ұйымдастыру – оларды сақтау, есепке алу және жою әрекеттерімен байланысты. Күрделі ақпараттық жүйеде бір пайдаланушы негізгі ақпараттың үлкен көлемімен жұмыс істей алады, соның әсерінен кейде негізгі ақпарат үшін шағын дерекқорларды ұйымдастыруды талап етеді. Мұндай жүйелер пайдаланылатын кілттерді қабылдау, сақтау, есепке алу және жоюға жауап береді. Пайдаланылған кілттер туралы ақпарат шифрланған түрде сақталу керек. Кілт туралы мәліметтерді шифрлайтын кілттер мастер-кілттер деп аталады және әдетте олар компьютер жүйесінде сақталмайды, оларды түрлендіру үшін криптографиялық алгоритмдер қолданылады. Пайдаланылатын кілттердің саны абоненттер санына, берілген ақпараттың көлемі мен шифрлау алгоритмінің ерекшелігіне байланысты. Бұл жағдайда сеанстық кілттер жойылуы қажет.

Кілттерді басқарудың үшінші мәселесі кілттерді жаңарту туралы сұрақпен тікелей байланысты – кілттерді тарату. Кілттерді тарату криптографияның негізгі міндеттерінің бірі болып табылады. Мәселенің ауқымын түсіну үшін, жеке мәліметтерді бір-бірімен алмастыратын n пайдаланушыларға қызмет көрсету кезінде $n(n-1)/2$ түрлі құпия кілттер қажет екенін көрсету қажет. Сонымен n өсуімен көптеген кілттерді басқару мәселесі туындайды. Оны шешудің бірнеше жолы бар. Ең қолайлысын анықтау келесі жағдайларға байланысты [9]:

- *Физикалық үлестіру.* Сенімді курьерлер немесе қарулы күзетшілердің көмегімен кілттерді дәстүрлі физикалық құралдармен жіберуге болады. Бұл процедура симметриялық немесе асимметриялық криптожүйелерде де қолданылады. Кілт

жасаушы қолданушыға асимметриялы құпия (немесе асимметриялық ашық кілтті) кілтті физикалық қауіпсіз түрде жібереді деп алдын ала белгіленеді.

- *Орталық кілт берушімен өзара әрекеттесу барысында қатысушылар ортақ кілт алады, яғни - «абоненттік шифрлау» схемасы.* Мұндай жүйеде кілттерді шығару және тарату орталығы жіберілген хабарламалардың шынайы және дұрыс екенінің кепілі болып табылады. Өйткені ол пайдаланушыларды кілттермен қамтамасыз етіп қана қоймай, сонымен қатар кілттерді жасауда және жеткізуде олардың құпиялығына жауап береді. Егер орталыққа зиян келтіріліп сенім жоғалса, кілттерге қатысты келесі сұраныстарды қамтамасыз етуде қиындық туады және бұрын берілген кілттердің қауіпсіздігі криптожүйеге байланысты болады.

- *Кілттерді сертификациялау орталығы арқылы пайдаланушылардың ашық кілттеріне қол жеткізу және құпия кілттерді беру.* Мұнда да симметриялық және асимметриялық криптожүйелер қолданылады. Пайдаланушы жұмыстың ең басында әр кілттерді тарату орталығымен қауіпсіз жолмен өзара байланысуы керек, сонда бұл бастапқы кілт алмасу жағдайында мәселенің бірі болып табылады. Егер ұзақ мерзімді құпия кілттер пайдаланушылар арасында және қандай да бір кілттерді тарату орталығы арасында таратылса, онда арнайы криптографиялық хаттамалар қолданылады. Таратудың бұл әдісінде пайдаланушылар және орталық «онлайн» режимінде жұмыс істеу ескеріледі.

- *Сенім желісі.* Асимметриялық криптожүйелерде қолданылады. Пайдаланушылар өз кілттерін таратады және басқа пайдаланушылардың кілттерін бақылайды. Кілттерді алмасудың бұл ресми емес түрінде сенім жатыр. Бір шешім, яғни әрбір пайдаланушыға сенім орталығымен байланыса алатын бір кілт бекітіледі. Бұл жағдайда n пайдаланушыларға арналған жүйе тек n кілтті қажет етеді. Екі пайдаланушы құпия мәлімет алмасқысы келгенде, олар осы хабарламаны жіберу үшін ғана пайдаланылатын кілт жасайды. Бұл *сеанс кілті* деп аталады. Сеанс кілті сенім орталығының қатысуымен хаттамалардың бірі арқылы жасалады.

- *Кілттермен алмасу хаттамасы.* Осы уақытқа дейін ортақ құпия кілті болмаған өзара қатысушылар арасында қорғалмаған байланыс арналары арқылы құпия кілт жасалады және алмасады. Ашық кілтті криптожүйелерді қолдана отырып, делдалдарға сенбейтін және кездесуге қабілетсіз серіктестер кілт айырбастау хаттамасына сәйкес желіде ортақ құпия кілтпен «онлайн» режимде келіссөз жүргізе алады. Бұл ашық кілтті шифрлау технологиясының ең көп қолданылатын түрі. Алдымен, тараптар алдын ала құпия кілтке келіседі. Содан кейін керекті ақпаратты шифрлау үшін келісілген кілтпен симметриялық шифр қолданылады.

Кілттерді орталықтан таратуды қолданатын әдістердің *кемшілігі* – орталық кімге және қандай кілттер тағайындалғанын біледі, ол ақпараттық жүйеде жүрген барлық хабарламаларды оқуға мүмкіндік береді. Кілттерді тікелей айырбастау кезінде субъектілердің түпнұсқалығын аутентификациялау проблемасы бар.

Сипатталған жүйелердегі кемшіліктерді есере отырып, заманауи талаптарға сай кілттерді басқару жүйесінің нұсқасын құру қарастырылды. Сонымен қатар, ұсынылған шифрлеу алгоритмдерінің ерекшеліктері ескеріледі.

Құрастырылған алгоритмнің бір ерекшелігі – бұл жүйеде кілт ретінде тек кездейсоқ сандар ғана емес, сонымен қатар жұмыс негізі болатын көпмүшеліктер де кілт ретінде алынады. Яғни, негізгі кілтке осы көпмүшеліктердің GF(2) өрісіндегі балама түрі де қосылады. Осыған байланысты бұл алгоритмдегі кілттер басқа алгоритмдерден қарағанда құрамдас болғандықтан толық кілт деп аталады. Бұл жүйеге арналған кілттерді басқаруда негізгі кілттерді генерациялаумен қоса осы аталған көпмүшеліктерді таңдау да қарастырылады.

Кілттерді басқаруды іске асыру симметриялық және асимметриялық біріктірілген криптожүйенің шеңберінде жүзеге асырылады. Осындай тәсілмен ашық мәтінді шифрлау және жіберу үшін ПЕПСЖ негізделген симметриялы криптожүйе пайдаланылады, ал симметриялық криптожүйенің құпия кілтін (толық кілтті) шифрлау, яғни толық кілтті шифрлау және жіберу үшін асимметриялық криптожүйесі қолданылады. Толық кілтпен шифрленген ақпаратпен бірге ашық кілттер жүүйесінде шифрленген.

Алдағы уақытта позициялық емес санау жүйелеріне негізделген ақпаратты шифрлеу алгоритмінің кілттерін басқару жүйесін жобалау және құрастыру жұмыстары жалғасын табатын болады.

Пайдаланылған әдебиеттер:

1. Амербаев В.М., Бияшев Р.Г., Нысанбаева С.Е. Применение непозиционных систем счисления при криптографической защите информации, // Изв. Нац. Акад. наук РК. Сер. физ.- мат. наук. – Алматы: Ғылым, 2005. – № 3. – С. 84-89.
2. Бияшев Р.Г., Нысанбаева С.Е. Формирование электронной цифровой подписи с проверяющими функциями // Комплексная защита информации: Матер. XI Междунар. конф. (20-23 марта 2007 г., Новополоцк, Республика Беларусь). – Минск: Амалфея, 2007. – С. 51-54.
3. Капалова Н.А., Нысанбаева С.Е. Алгоритм открытого распределения ключей на базе непозиционной полиномиальной системы счисления // Вестник КазНУ. Сер. мат., мех., информат. - 2007. - №3 (54), - С. 82-87.
4. Biyashev R., Nyssanbayeva S., Kapalova N., Haumen A. Modified symmetric block encryption-decryption algorithm based on modular arithmetic // Proceedings of the International Conference on Wireless Communications, Network Security and Signal Processing (WCNSSP 2016). – Chiang Mai, Thailand, 2016. –P. 263-265. (Web of Science, Thomson Reuters)
5. Капалова Н.А., Хаумен А. Алгоритм шифрования на SP-сети // Материалы научной конференции Института информационных и вычислительных технологий МОН РК «Современные проблемы информатики и вычислительных технологий». – Алматы, 2017. – С. 113-118.
6. Фомина И.А. Управление ключами в криптографических системах. Вестник Нижегородского университета им. Н.И. Лобачевского. 2010, №4(1), стр.165-169.
7. Аристархов И.В. дисс. Управление сертификатами ключей проверки электронной подписи, Москва, 2012
8. Кнут Д.Э. Искусство программирования. Т.2. Получисленные алгоритмы. М.:Издательский дом «Вильямс», 2004. 832 с.
9. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексы на языке Си. М.: Из-во «Триумф», 2003. 816с.

ЖҮЙКЕ ЖҮЙЕСІНІҢ ҚҰРЫЛЫМЫ МЕН ҚАСИЕТТЕРІН ИМИТАЦИЯЛАЙТЫН НЕЙРОНДЫ ЖЕЛІЛЕР

Қожахмет Б.[1,2], Калижанова А.У.[1,2]

ҚР БҒМ ҒК, Ақпараттық және есептеуіш технологиялар институты,
e-mail: *banu_kozhakhmet@mail.ru*

СОДЕРЖАНИЕ