ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

5) общего и среднего времени выполнения программ от заданного преподавателем параметра одной или нескольких станций или линии связи;

6) количества столкновений от заданного преподавателем параметра одной или нескольких станций или линии связи.

Список использованных источников

1) Таненбаум Э.С. Архитектура компьютера, 4-е издание. С-Пб: Изд. Питер, 2003. 704 с.

2) Столингс У. Структурная организация и архитектура компьютерных систем, 5-е издание. М: Изд. дом Вильямс, 2002. 896 с.

3) Локальные вычислительные сети. Справочник. Под ред. С.В. Назарова М.: Финансы и статистика, 2007. – 58 с.

УДК621.316.97

ЭЛЬ – ГАМАЛЬ ЖӘНЕ RSA АЛГОРИТМДЕРІНІҢ ЭЛЕКТРОНДЫ САНДЫҚ ҚОЛТАҢБАЛАРЫНЫҢ ҚАЗАҚСТАНДАҒЫ ҚОЛДАНЫСЫ

Алдашева Лаура Сабитхановна
aldasheva_ls@enu.kz
Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникациялар кафедрасының аға оқытушысы, Астана, Қазақстан
Майлыбаева Гульжас Жаксылыковна
gul_zhas@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Радиотехника, электроника және телекоммуникациялар кафедрасының оқытушысы, Астана, Қазақстан

Қазіргі ғылым мен техника қатар дамыған заманда криптографиялық жүйелер құпия ақпаратты оңай тасымалдау үшін қолданылады. Соның бір мысалы, электронды сандық қолтаңбаны қолданып, қағазсыз құжат айналымында дәстүрлі мөрді және қол қоюды ауыстыру болып табылады. Бұл жүйені қолданудың ең тиімді жақтарының бірі қаржылық шығындарды аз болуы мен уақыттың үнемді жұмсалуында. *Электрондық сандық қолтаңба* – уақыттың жаңа талаптарымен бірге қадам басуды қалағандардың барлығы үшін тиімді шешім. Оны *жасанды көшіру мүмкін емес*.

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.

Электронды сандық қолтаңба алгоритмі екі топқа бөлінеді:

- Қарапайым сандық қолтаңба
- Құжатты қалпына келтіретін сандық қолтаңба

Қарапайым сандық қолтаңбаға ГОСТ Р34.10-2001, ДСТУ, ECDSA стандарттары жатады.

Құжатты қалпына келтіретін сандық қолтаңбаларда қол қойылатын құжат болады: қолтаңбаны тексеру барысында автоматты түрде құжат та есептелінеді. Өте танымал алгоритмдердің бірі RSA осы топқа жатады.

Электронды сандық қолтаңбаны жасау үшін әртүрлі алгоритмдер қолданылады, олар: сандық қолтаңбаның RSA алгоритмі, сандық қолтаңбаның стандарттары және технологиялар ұлттық институтының DSA алгоритмі, Эль-Гамаль криптожүйесі, Окамото алгоритмі ESIGN, Шнорр сандық қолтаңбасы, Микали-Шамир цифрлы қолтаңбасы, ГОСТ Р34.10-94 және Р34.11-94 сандық қолтаңбасы, «Нотариус» сандық қолтаңбасы.

Осы алгоритмдердің ішінде ең сенімдісін, қауіпсізін анықтау мақсатында RSA және Эль – Гамаль алгоритмдерін салыстыруға болады. RSA және Эль-Гамаль криптожүйелері бір – біріне өте қатты ұқсайды.

RSA және Эль-Гамаль алгоритмдері пайдаланушылардың бір-бірімен өте тығыз байланыста болғандарын қажет етпейді. RSA алгоритмінің қауіпсіздігі құрамына санның жіктелуінің қиындығына, ал Эль-Гамаль хаттамасының қауіпсіздігі дискретті логарифмнің күрделі есептеуіне негізделген [1]. Бұл алгоритмдердің негізгі салыстырмалы қасиеттері 1- кестеде келтірілген.

RSA алгоритімінде, егер (e) шифрлау көрсеткіші аз сан болса, онда хабарды кілтсіз бұзып оқу қаупі орын алады. Екі жақтағы қолданушылар n модулінің жалпы мәнін бірдей қолданса, онда олардың құпия кілттерінің өзара ашылуына әкеледі[2].

Эль-Гамаль хаттамасында кілтсіз бұзып оқу орын алмауы үшін кез келген k сандарын болжап таба алмайтындай және қайталанбайтындай болуы қажет [3].

1-кесте. RSA, Эль – Гамаль алгоритмдерін қасиеттері бойынша салыстыру

Алгоритм	RSA	Эль – Гамаль
Кілт	4096 битке дейін	4096 битке дейін
Қолданылуы	Шифрлау және қолтаңба	Шифрлау және қолтаңба
Криптотөзімділік, MIPS	1300 бит кілті үшін $2{,}7 \bullet 10^{28}$	Кілттің ұзындықтары бірдей кезде, RSA криптотөзімділігіне тең, яғни $2{,}7 \bullet 10^{28}$
Ескертпелер	Үлкен сандарды жіктеудің қиыншылығының негізінде құрылған. Ассиметриялық алгоритмдердің алғашқыларының бірі. Көптеген стандарттарға қосылған.	Соңғы өрістегі дискреттік логарифмдерді есептеудің қиыншылығына негізделіп құрастырылған. Кілттерді төзімділікті төмендетпей тез генерациялауға мүмкіндік береді. DSS стандартындағы DSA сандық қолтаңба алгоритмінде қолданылады.

Эль – Гамаль алгоритмінің ЭСҚ-сы

Бір хабарлама екінші рет қайта жазылғанда электронды сандық қолтаңба әртүрлі болуы үшін Эль-Гамаль келесі алгоритмді ұсынды.

Эль – Гамаль сандық қолтаңбасы қасиеттері жағынан өзіне ұқсас басқа қолтаңбаларының жасалуына әсер етті. Оның негізінде келесі салыстыру жатыр: $y^A a^B = g^C (\mathrm{mod}\, \rho)$, мұндағы A, B, C үштігі қандай – да бір белгіні таңдағанда келесі ауыстырулардың бірін қабылдайды $\pm a, \pm b, \pm H$. Мысалы, Эль – Гамальдың бастапқы схемасы $A=a$, $B=b$, $C=H$ болады.

Осы принциптер негізінде АҚШ және Ресейде электронды сандық қолтаңбалар жасалған:

- Американдық DSS (Digital signature standard) стандартынды $A=a$, $B=-b$ мәні қолданылады.
- Ресейлік стандартта $A=-a$, $B=-H$, $C=b$. Қазір Ресейде 2001 жылы қабылданған жаңа ГОСТ Р34.10-2001стандарты қолданылады.

Эль – Гамаль алгоритмі бұл тізбекте ең қарапайым болып көрінгенімен, жеткілікті түрде криптотөзімді болып табылады [4].

Эль – Гамаль алгоритмінің ЭСҚ – сының артықшылықтары

1. Есептеу кезіндегі сандар бірдей төзімділік дәрежесінде әдеттегіден 25% - ке азырақ болады. Соның нәтижесінде есептеу қиыншылықтарын екі есеге дейін азайтуға мүмкіндік береді [3].

2. RSA электронды сандық қолтаңбасындағыдай, жаңа хабарлама келгенде, оның жасырын кілтін білмей тұрып, электронды қолтаңбасын есептеуге болмайды.

3. Эль – Гамаль алгоритміне бір үлкен Р жай саны жетеді, ал RSA алгоритміне екеуі керек [3].

Мысалы: $p = 11$ және $g = 2$ домен параметрлері. Хабарламаны жіберушінің жасырын кілті $x = 8$. Ашық кілттің үшінші санын есептеп тауып, хэш $H = 5$ болатын, М хабарламаға қол қою керек.

Шешімі: $y = g^x \bmod p = 2^8 (\bmod 11) = 3$. Ашық кілт (11, 2, 3). $H(M) = 5$ хабарлама хэші. Рандомизатор $r = 9$-ға тең болсын.

$$a = g^r (\bmod p) = 2^9 (\bmod 11) = 6$$

$$b = (H - ax) r^{-1} (\bmod p - 1) = (5 - 6 \cdot 8) \cdot 9^{-1} (\bmod 10) = 3 (\bmod 10)$$

Қолтаңба (6, 3). Қол қойылған (М, 6, 3) хабарлама қолданушыға жіберіледі. Хабарламаны алушы қолтаңбаны тексеруден өткізеді. Хэшті тауып, 2 санды есептеп шығарады, ашық кілттің барлық үш бөлігін біліп алады.

$$y^a a^b (\bmod p) = 3^6 \cdot 6^3 (\bmod 11) = 10;$$

$$g^H (\bmod p) = 2^5 (\bmod 11) = 10.$$

Бұл сандар дәлме-дәл шықты, демек хабарлама түпнұсқа.

RSA алгоритмінің ЭСҚ – сының артықшылығы Эль – Гамаль алгоритмінің ЭСҚ – сының кемшілігі болып табылады: Эль – Гамаль электронды сандық қолтаңбасында сандық қолтаңбаның ұзындығы RSA алгоритмінен 1,5 есе көп. Бұл есептеу уақытын ұзартады [1].

RSA алгоритмінің ЭСҚ-сының кемшіліктері:

1. Кілтті таңдау кезінде, көптеген қосымша шарттарды тексеру қажет. Бұл практикалық түрде қиындыққа әкеліп соқтырады. Осы шарттардың бірі орындалмаған жағдайда, криптоаналитик тарапынан сандық қолтаңба бұрмалануға ұшырайды. Тіпті теориялық тұрғыда да маңызды құжаттарға қол қою кезінде, қосымша шарттар бұзылмауы керек.

2. DES(10^{18}) шифрлау жүйесі секілді электронды сандық қолтаңбаның криптотөзімділігін қамтамасыз ету үшін, 2^{512} (немесе 10^{154}-ге жуық) сандар тәртібін қолдану керек. Ол есептеуге үлкен шығындар әкеледі.

3. RSA электрондық сандық қолтаңбасы мультипликативті шабуылдарға қарсы тұру қабілеті осал [1].

Мысалы: $n = 784319$ және $e = 313$ А қолданушының ашық кілттері, $d = 160009$ жабық кілті. $x = 19070$ Б қолданушыға жеткізілуі тиіс қол қойылған хабарлама.

Шешімі:

$$S = (19070)^{160009} (\bmod 784319) = 210625$$

$x = 19070$ және $S = 210625$ жұбы Б қолданушыға жіберіледі. Қолтаңбаны тексер үшін, Б қолданушы А қолданушының ашық кілтінен келесіні табады:

$x' = (210625)^{313} (\bmod 784319) = 19070 = x$ хабарламасы заңды.

Ұзақ хабарламаға қол қою үшін, оны блоктарға бөліп, әр блокка жеке – жеке қол қойып шығу керек. Әрине, бұл ұзақ уақытты қажет етеді.

Қазақстан Республикасының 2003 жылы 7 қаңтарда қабылданған «Электрондық құжат және электронды сандық қолтаңба туралы» заңында «тіркелу куәлігі»

түсінігі берілген. Ол халықаралық тәжірибеде «сертификат» немесе «ашық кілттің сертификаты» ретінде қолданылады.

Қолтаңба Қазақстан Республикасының барлық азаматтары мен азаматшалары үшін қолжетімді.

E-gov электронды үкіметі порталынан алынған сертификатты ашу үшін RSA сертификаты ұсынылады. Халыққа не үшін RSA сертификаты ұсынылады?

- ЭСҚ-ны 2012 жылдың 30 сәуіріне дейін алған ескі қолданушылар үшін: GOST сертификаты сұранысқа қол қою үшін, ал RSA порталдағы аутентификация үшін арналған.
- ЭСҚ-ны 2012 жылдың 1 мамырынан алған жаңа қолданушылар (жеке тұлғалар) үшін: RSA сертификаты сұранысқа қол қою үшін, ал AUTH_RSA порталдағы аутентификация үшін арналған.
- Жаңа қолданушылар үшін (заңды тұлғалар): GOST сертификаты сұранысқа қол қою үшін, ал RSA порталдағы аутентификация үшін арналған.

Еліміз қазіргі күні ақпараттық технологиялар заманы көшінің соңында қалып отырған жоқ. Біріккен Ұлттар Ұйымының электронды үкіметті дамыту жөніндегі рейтингінде еліміз былтырғы жылы 193 мемлекеттің арасынан 28-ші сатыға жайғасты. Бұның алдындағы жылы ел аталған рейтинг бойынша 38-ші орында тұрған еді.

Қазіргі таңда Қазақстан Республикасында 2,4 млн ЭСҚ шығарылған, соның 500000-ы азаматтардың жеке куәліктерін алмастыра алатын ID картада жазылған. Әрі қарай ЭСҚ-ны мобильді құрылғылардың сим картасына жазу жоспарға алынған. ЭСҚ берілуінің мобильді платформасы Қазақстанда 2014-2016 жж құрылады. Мобильді үкімет – Қазақстан Республикасының электронды үкіметінің дамуының жаңа кезеңі.

Қазір еліміздегі 570 мемлекеттік қызмет электрондық түрде көрсетіледі, барлық лицензиялар электрондық форматта беріледі.

Қорытындылай келе, салыстырылған екі алгоритмнің сандық қолтаңбаларының ең сенімдісі ретінде Эль-Гамальді айтуға болады. Жоғарыда айтып өткендей, Эль – Гамаль алгоритмі де кемшіліксіз емес, RSA алгоритмінің артықшылығы – соның дәлелі. Әлем елдерінің біразы, соның ішінде Қазақстан Республикасы да RSA алгоритмін ЭСҚ ретінде қолданады.

Қолданылған әдебиет

1. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В Основы криптографии. – М.: Гелиос АРВ, 2002, 480 с.

2. Коутинхо С. Введение в теорию чисел алгоритм RSA. – М.: Постмаркет, 2001, 328с.

3. Фороузан Б.А. Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.

4. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone 11.5.2 The ElGamal signature scheme // Handbook of applied cryptography.

УДК 621.391

ИСПОЛЬЗОВАНИЕ АЛГОРИТМ ПРИМА ДЛЯ РАСЧЕТА СЕТИ ДОСТУПА МИНИМАЛЬНОЙ СТОИМОСТИ

Беков Нурсултан Кабжанулы
Nursultan_bekov@mail.ru
Магистрант группы МРЭТ-22 ЕНУ им.Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Ш.Ж.Сеилов