ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ КН МОН РК

ӘЛ-ФАРАБИ атындағы ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

TURAN UNIVERSITY

МАТЕРИАЛЫ

II МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ

«ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА»

«ИНФОРМАТИКА ЖӘНЕ ҚОЛДАНБАЛЫ МАТЕМАТИКА

«COMPUTER SCIENCE AND APPLIED MATHEMATICS»

(ЧАСТЬ II)

Алматы

27-30 сентября 2017 года

www.conf2017.ipic

КРИПТОГРАФИЯЛЫҚ ПРОТОКОЛ

Вуйцик В.[1], Ахметова А.М.[2], Нугманова С.А.[2]
ardak_66@mail.ru, nugm_s@mail.ru

[1] *Institute of computer science of the Lublin Technical University Lublin University of Technology*
[2] *Ақпараттық және есептеуіш технологиялар институты*

Аңдатпа. *Мақалада криптографиялық протокол ұғымы қарасырылған. Оның қасиеттері анықталып, олардың типтері шартты екі топқа бөлінген. Кейбір протокол түрлерінің міндеттері сипатталған. Негізгі терминдерге шолу жасалды.*

Кілттік сөздер. *Криптографиялық протокол, кілт, криптоталдау*

Казіргі таңдағы ақпараттық технологияларды мемлекеттік және қаржылық салаларда, сондай-ақ қоғамда кеңінен қолдағандықтан ақпараттық қауіпсіздік мәселелердің шешудің негізгілердің бірі. Ақпараттандыруда ақпараттың жайылып кету мүмкіндігінен болатын тікелей залалдан басқа адамның бостандығын басу, тұлғаның рухани және мемлекеттік өмірінде қатерлі қауып көзіне айналуы мүмкін.

1977 жылы АҚШ-та алғаш мәліметтерді шифрлеу стандарты Data Encryption Standard (DES) қабылданды. Ол 1980 жылы АҚШ Ұлттық стандарттар және технологиялар институтымен (Mationl Linstitut of Standards and Technologyб NIST) стандарт ретінде қабылданды. Стандарт АҚШ мемлекеттік және коммерциялық мекемелердегі құпия емес, бірақ ақпараттарды рұқсатсыз қол жеткізуден қорғау үшін қолданылады [1]. Стандарт алгоритмі Фейстель сызбасы мен Керсхоффс қағидасы бойынша құралған.

1976 жылы криптографиялық жүйелер екі салаға бөлінді-симметриялы (жабық кілті) және асимметриялы (ашық кілті), осы жылы У.Диффи мен М.Хеллманның ашық кілтті криптография қағидаларын сипаттаған еңбегі жарияланды [2-5]. Дәстүрлі шифрлеу әдістерін қолданып ақпаратты қорғаудың түрлі әдістері мен құралдардың тиімділігін құруда және тәжірибеде қолдану бойынша алыс және жақын шетелдерде жеткілікті тәжірибелері бар. Мәліметтері шифрлеу алгоритм стандарттары бар елдер, ақпараттық-коммуникациялық технологиялық құралдарын басқа елдерге экспортқа шығарғанда, криптотұрақтылығы әлдеқайда төмен бағдарламалық бұйымдарға қолданылмайды. Сондықтан Қазақстанға ақпараттық қауіпсіздікті қамтамасыз ету үшін басқа да қаржыландыру көздерін жұмылдыру өзекті қажеттілік болып тұр. Бұл мәселе бүкіл ТМД елдерінде, сонымен қатар Рессейде де кездеседі.

Казіргі таңда жаңа тиімді криптографиялық алгоритмдерді іздестіруге жақын және алыс шетелдерде қызығушылық арта түсуде. XX ғасырдың 70-80

жылдарында құралған алгоритмдер оларды жүзеге асыру кезіндегі тиімділік талаптарына сай болу керек еді. Казіргі таңда шифрлеуды жүзеге асыру бойынша техникалық базаның мүмкіндігі өткен ғасырдың 70-ші, 80-ші жылдарға қарағанда бірнеше есе артқан. Осының нәтежесінде оларға криптоталдау жасау мумкіндігі пропорцияналды ұлғайды, және соның салдарынан, криптотұрақтылыққа деген талаптар күшейтілді [6]. Құпиялы кілтті блоктық шифрлауға деген замани тәсілдердің өзгеруі осыған байланысты.

2002 жылдың мамырында АҚШ конкурс нәтежесі бойынша жаңа шифрлеу стандарты AES қабылданды. Алдыңғы алгоритмдерден айырмашылығы AES құру кезінде оның өзгертулерінде алгебралық тәсіл кеңінен қолданылды. Еуропалық одақта конкурсты құрылымы «салынған» Фейстель сызбасына негізделген алгоритм жеңді. Бұл конкурстар криптография мен крипто анализдің қортынды дамуына қатты ықпал етті.

Ресейде ақпараты өңдеу жүйелерінде мәліметті криптографиялық өзгерту үшін стандарт ГОСТ 28147-89 қолданыста. Оны қолдану Ресейдің мемлекеттік және бірқатар коммерциялық мекемелерде міндетті болып табылды. Беларусь Республикасында 2011жылы BelT-СТБ34.101.31-2007 "Ақпараттық технология және қауіпсіздік. Шифрлеу және тұтастықты қадағалау криптографиялық алгоритмдері" тұтастықты қадағалау және симметриялы шифрлеу стандарты қабылданды [7].

Біздің республикамызда заманауи ақпараттық технологиялар қарқынды құрылып және ендіріліп жатыр – «е- технологиялар». Осыған байланысты электронды қарым қатынас кезінде ақпараттық қауіпсіздікті қамтамасыздандыратын, тиімді және тұрақты құралдарға деген қажеттілік арта түседі. Қарастырылып отырған зертеу жұмысымда шифрлау алгоритмдері мен электронды сандық алгоритмдер зерттелін және құрылды, құрылған алгоритмдер мен әдістер позициялық деп аталды. Кілттің ұзындығы-криптотұрақтылығының бір белгісі. Құрылған шифрлеу және сандық қолтаңба жүйелерінде криптотұрақтылық критерий ретінде, толық кілтпен сипатталатын, сол шифрлеу және сандық есептеу алгоритмдерінің криптотұрақтылығын қолдану ұсынылған.

Оның құрамына стандартты құпия кілттен басқа модулдік арифметика негізінде құралған криптоалгоритмдердің құпия параметрлері де кіреді. Қазақстанда көрсетілген тақырып бойынша басқа мекемелерде зерттеулер жүргізілмейді. Ашық басылымдар бойынша қарасақ ұсақ зерттеулер басқа елде де жоқ [8].

Қазіргі криптографияда шифрлерді жасаудан және зерттеуден басқа криптографиялық протоколдарды әзірлеуге көп назар аударылады.

Криптографиялық протокол – криптографиялық құралдарды пайдаланып екі немесе одан көп абоненттердің өзара әрекеттесу процедурасы, оның нәтижесінде абоненттер өзінің мақсатына жетеді, ал олардың қарсыластары – жетпейді. Протоколдың негізінде ақпараттық процестердегі криптографиялық өзгерістер мен алгоритмдердің пайдалануын регламенттейтін ережелер

жиынтығы жатыр. Әрбір криптографиялық протокол белгілі бір есепті шешуге арналған.

Кез келген протоколдың келесі қасиеттері бар [9]:

протоколды орындаған кезде іс-әрекеттің реті маңызды; әрбір іс-әрекет алдағы аяқталғаннан кейін өзінің ретімен орындалу керек;

протокол қайшы болмау керек;

протокол толық болу керек, яғни әрбір мүмкін болатын жағдайы үшін сәйкес іс-әрекет ескерілу керек.

Протокол қасиеттері информатикадан белгілі алгоритм қасиеттеріне ұқсайды. Шынында да, протокол – бұл белгілі жағдайда бірнеше тараптардың іс-әрекеттесу алгоритмы. Протокол қатысушылары протоколды білу керек және оның барлық кезеңдерін толық орындау керек. Криптографиялық протоколдың қатысушылары әдетте кейбір байланыс жүйенің абоненттері. Протокол қатысушылары бір біріне сенбеу мүмкін, сондықтан криптографиялық протоколдар оның қатысушыларын сыртқы жаудан ғана емес, серіктестердің арамдық іс-әрекетінен де қорғау керек.

Криптографиялық протоколдардың типтерін шартты екі топқа бөлуге болады [10]: қолданбалы және қарадүрсін протоколдары. Қолданбалы протокол тәжірибеде кездесетін нақты есепті шешуге арналған. Қарадүрсін протоколдар қолданбалы протоколдарды әзірлеген кезде «құрылыс блоктар» сияқты пайдаланады. Біз оқу құралында тек қарадүрсін протоколдарды қарастырамыз.

Кейбір протокол түрлерінің міндетін қарап шығайық.

1. *Хабарларды конфиденциал беру протоколы*. Хабарларды конфиденциал берудің міндеті келесі. Байланыс желінің абоненты болатын протоколдың екі қатысушысы бар. Қатысушылар кейбір байланыс жолымен қосылған, ол бойынша хабарды екі жаққа жіберуге болады. Байланыс жолды қарсылас бақылау мүмкін. Абоненттің біреуінде конфиденциал хабар m бар, осы хабарды конфиденциал түрде екінші абонентке беру керек. Осындай протокол тіпті бірінші пайда болған.

2. *Аутентификация және идентификация протоколдары*. Олар кейбір ақпаратқа рұқсатсыз қатынауды және пайдаланушылардың өкілеттігі жоқ қорларға қатынауды болдырмауға арналған. Кәдімгі қолдану саласы – кейбір үлкен ақпараттық жүйенің қорларына пайдаланушылардың қол жетімділігін ұйымдастыру.

3. *Кілттерді үлестіру протоколы* – шифрланған хабарлармен алмасудағы қатысушыларды құпиялы кілттермен қамтамасыз ету үшін қажетті.

4. *Электронды цифрлық қол протоколы* – қағаз құжаттардағы кәдімгі қол сияқты электронды құжаттарға қол қоюға мүмкіндік береді. Протокол орындалу нәтижесінде, берілетін ақпараттың авторлық тексеруін қамтамасыз ететін, оған бірегей сандық қосымша қосылады.

5. *Қадағалмауды қамтамасыз ететін протоколы* («Электронды ақша»). Криптографияда электронды ақша деген қадағалмауды қамтамасыз ететін (яғни

ақпаратты тасымалдау көзін қарап жүруге мүмкін еместігі) электронды төлем құралдарды айтады.

Екі тараптың арасында конфиденциал хабарлармен алмасудың қарапайым протоколын қарастырайық, тараптарды абонент №1 және абонент №2 деп атайық. Абонент №1 шифрланған хабарды абонент №2 –ге бергісі келсін. Бұл жағдайда олардың іс-әрекет тізбегі мұндай болу керек [11].

1. Абоненттер шифрлау жүйесін таңдайды (мысалы, *n* позицияға жылжытуы бар Цезарь шифры).

2. Абоненттер шифрлау кілті туралы келіседі.

3. Абонент №1 бастапқы хабарды таңдалған әдіс арқылы кілт көмегімен шифрлайды және шифрланған хабарды алады.

4. Шифрланған хабар абонент №2 –ге жіберіледі.

5. Абонент №2 шифрланған хабарды кілт көмегімен ашады және ашық хабарды алады.

Бұл протокол оңай, бірақ ол шынында тәжірибеде пайдалану мүмкін. Криптографиялық протоколдар міндетіне байланысты қарапайым да күрделі де болу мүмкін.

Алдында біз криптографиялық шабуыл анықтамасын енгіздік және криптографиялық алгоритмге шабуылдар типтерін қарап шықтық [12]. Көп жағдайда шабуыл шифрлау алгоритмге емес протоколға бағытталу мүмкін. Сондықтан, абсолют сенімді шифрлау алгоритмының бар болуы байланыс жүйенің абоненттеріне толық қауіпсіздікті кепілдей алмайды. Сол себептен қазіргі уақытта мамандар криптографиялық протоколдарды ұқыпты талдайды.

Негізгі терминдер [13]

Ciphertext – шифрланған хабар (жабық мәтін, криптограмма).

Deciphering – шифрды ашу (дешифрлау).

Enciphering – ашық мәтінді криптограммаға түрлендіру (шифрлау).

Plaintext – бастапқы хабар немесе ашық мәтін.

Белсенді криптографиялық шабуыл – осындай шабуылда қарсылас берілген хабарларды өзгерте алады және өзінің хабарларын қоя мүмкін.

Әліпби (алфавит) – ақпаратты кодтау үшін пайдаланатын символдардың шекті көптігі.

Кілт – хабарларды шифрлауға және дешифрлауға қажетті ақпарат.

Криптоталдау – ақпараттың криптографиялық қорғауын жеңіп алу туралы ғылым.

Ақпаратты қорғаудың криптографиялық жүйесі – деректерді шифрлау үшін криптографиялық әдістерді пайдаланатын ақпаратты қорғау жүйесі.

Криптографиялық протокол – криптографиялық құралдарды пайдаланып екі немесе одан көп абоненттердің өзара әрекеттесу алгоритмы, оның нәтижесінде абоненттер өзінің мақсатына жетеді, ал олардың қарсыластары – жетпейді.

Криптография шифрлау жүйелерінің құруын және пайдалануын зерттейді, соның ішінде түрлі ашу әдістер жөнінде олардың беріктігін, осал жерін және осалдық дәрежесін.

Криптобериктік – кілтті білмегенде дешифрлауға беріктікті анықтайтын шифр сипаттамасы (яғни криптоталдауға қарсы тұру қабілеті).

Пассивті криптографиялық шабуыл - қарсыластар берілетін хабарламаны өзгертуге мүмкіндігі болмағандағы шабулы. Пассивті шабуыл кезінде берілетін хабарларды тек тыңдауға, дешифрлауға және трафикті талдауға болады.

Керкхоффс принципы – криптографиялық жүйелерді құрастыру ережесі оған сәйкес құпиялы түрде шифрлау кілті сақталынады, ал шифрлау жүйесінің басқа параметрлері, алгоритмның беріктігін төмендетпей, ашық та болу мүмкін. Басқа сөзбен, 24 шифрлаудың сенімділігін бағалаған кезде қарсылас пайдаланатын шифрлау жүйесі туралы, қолданылатын кілттерден басқа, бәрін біледі деп ойлаймыз. Бұл принципті XIX ғасырда алғаш тұжырымдаған голланд криптографы Огюст Керкхоффс.

Символ – кез келген белгі, соның ішінде әріп, цифр немесе тыныс белгісі.

Шифрлау жүйесі немесе шифржүйесі – хабардың мәтінің қайтымды өзгерту үшін (жолданған адамнан басқа барлықтарға мәтін түсініксіз болсын деп) пайдаланатын кез келген жүйе.

Шифр – бастапқы құпиялы хабарды қорғау үшін оның алдын ала айтылған түрлендіру тәсілдерінің жиынтығы.

Жабық кілті бар шифрлау (симметриялық шифрлау) - деректерді қайтымды түрлендіру әдісі. оларда ақпараттық алмасудың екі жағы да жаудан жасырын сақтайтын бір кілтті ғана пайдаланады. Тарихтан танымал барлық шифрлар мысалы Цезарь шифры – бұл жабық кілті бар шифрлар.

Ашық кілті бар шифрлау (ассимметриялық шифрлау) - деректерді шифрлау және дешифрлау үшін екі әртүрлі кілтті пайдаланатын шифрлау әдістері. Мұнда кілттердің біреуі (ашық кілт) ашық (қорғалмаған) арна арқылы берілу мүмкін.

Электронды (цифрлық) қол - криптографиялық түрлендіру көмегімен алынған хабарға қосылатын деректер блогы [14]. Мәтінді алған кезде электрондық қол хабардың авторлығы мен нақтылығын тексеруге мүмкіндік береді.

Әдебиеттер

1 *Червяков Н.И.* Применение системы остаточных классов в цифровых системах обработки и передачи информации. – Ставрополь: СВВиУС, 1984.

2 *Акушский И.Я.* Многорегистровые схемы выполнения арифметических операций. «Вопросы теории математических машин». Физматгиз,1958.

3 *Акушский И.Я.* Арифметические операции в системе остаточных классов. «Вопросы радиоэлектроники», 1960г.

4 *Акушский И.Я., Хацкевич В.Х.* Инверсные представления чисел в системе остаточных классов. «Цифровая вычислительная техника и программирование», вып. 2,1967г.

5 *Акушский И.Я., Юдицкий Д.И.* Позиционные характеристики числовых представлений в остаточных классах. «Цифровая вычислительная техника и программирование», вып. 2,1967г.

6 *Акушский И.Я., Юдицкий Д.И.* Некоторые вопросы логики и структуры УЦВМ высокой пройзводительности.«Вопросы радиоэлектроники», серия 1960г., вып. 3.

7 *Анисимов Б.В., Четвериков В.Н.* Основы теории и проектирования цифровых вычислительных машин. Машгиз,1962.

8 *Виноградов И.М.* Основы теории чисел. Изд-во «Наук»,1965.

9 *Геллер С.И., Долгов А.И.,Золин В.В.* Алгоритмы основых операций в системе счисления остаточных классов и их реализации.Всборнике «Вопрос построения быстродействующих ЦВМ».АРТА.Харьков.1965.

10 *Жуков-Емельянов О.Д.* Некоторые вопросы.связанные с умножением и делением в системе остаточных классов. ИТМ и ВТ. Электронные вычислительные машины.1964.

11 *Жуков-Емельянов О.Д.* Цепной алгоритм в системе остаточных классов.ИТМ и ВТ. Электронные вычислительные машины.1965.

12 *Файн С.Б.* Некоторые вопросы машинной арифметики системе остаточных клапанов.Труды ВЦ АН Груз.ССр,1964.

13 *Дроздов Е.А., Пятибратов Ф.П.* Автоматическое преобразование и кодирование информации. Изд-во «Советское радио», 1964.

14 *Дэвенпорт Г.* Высшая арифметика. Изд-во «Наука» 1965.

ПОЗИЦИЯЛЫҚ ЕМЕС САНАУ ЖҮЙЕСІ НЕГІЗІНДЕ ҚҰРЫЛҒАН ЭЛЬ-ГАМАЛЬ ШИФРЛАУ АЛГОРИТМІН МӘЛІМЕТ АЛМАСУ ЖЕЛІСІНДЕ ПАЙДАЛАНУ

Хомпыш А.
ardabek@mail.ru

ҚР Білім және ғылым министрлігі Ғылым комитетінің «Ақпараттық және есептеуіш технологиялар институты»

Аңдатпа. *Бұл мақалада позициялық емес санау жүйесі негізінде құрылған Эль-Гамаль шифрлау алгоритмінің тиімділігін зерттеу үшін, MYCLIENT сұхбаттасу қосымшасына қолдану бойынша талқыланды.*