ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н.ГУМИЛЕВ атындағы ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ им. Л.Н.ГУМИЛЕВА

ЖАС ҒАЛЫМДАРДЫҢ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯСЫ «ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2009»

МЕЖДУНАРОДНАЯ НАУЧНАЯ КОНФЕРЕНЦИЯ МОЛОДЫХ УЧЕНЫХ «НАУКА И ОБРАЗОВАНИЕ - 2009»

ЖАС ҒАЛЫМДАРДЫҢ ХАЛЫҚАРАЛЫҚ
КОНФЕРЕНЦИЯСЫНЫҢ ЕҢБЕКТЕРІ
29-30 сәуір 2009 жыл.

ТРУДЫ МЕЖДУНАРОДНОЙ НАУЧНОЙ КОНФЕРЕНЦИИ
МОЛОДЫХ УЧЕНЫХ
29-30 апреля 2009 года.

І БӨЛІМ
ЧАСТЬ I

Астана, 2009

ББК

Жалпы редакцияны басқарған з.ғ.д., профессор Б.Ж. Әбдірайымов
Под редакцией д.ю.н., профессора Б.Ж. Абдраимова

«Ғылым және білім - 2009» халықаралық жас ғалымдар конференциясының материалдар жинағы. – Астана, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2009. 1 бөлім, - 470 б.

Сборник материалов международной научной конференции молодых ученых «Наука и образование - 2009».– Астана, Евразийский национальный университет им. Л.Н. Гумилева, 2009. 1 часть, - 470 с.

Жинаққа студенттердің, магистранттардың, аспиранттардың және PhD докоранттардың жаратылыстану-техникалық және гуманитарлық салаларындағы өзекті мәселелері бойынша еңбектері енгізілген.

В сборник вошли материалы студентов, магистрантов, аспирантов и докторантов PhD по актуальным вопросам естественно-технических и гуманитарных наук.

ББК

ISBN

Жинақты баспаға шығару жұмысына қатысқандар:
В подготовке сборника к печати принимали участие:
Аджиханова А.(ФТФ), Аскарбекова А.(ФТФ), Байбосынова Л.(ИСФ), Жаксыгулова А.(ФТФ), Махашева А.(ФМИТ), Мухышбаева А.(ФТФ), Рахметова Г.(ФМИТ), Сырлыбаева Г.(ФТФ), Шалимова Н.(ФМО).

Тексты тезисов печатаются в авторской редакции
Тезис тексттері авторлық редакцияда баспаға шығарылады

СОДЕРЖАНИЕ
МАЗМҰНЫ
I Бөлім/ I Часть

Следствие. *При условии теоремы имеет место неравенство*

$$\left(\sum_{m=D}^{\infty}\sum_{n=D}^{\infty}\gamma_{mn}\left|\hat{f}(m,n)\right|\right)^{r} \le kCV_s^{r/2}(f)\sum\sum(m,n)^{-r}\gamma_{mn}\omega^{(2-s)r/2}(f;\frac{1}{m};\frac{1}{n}).$$

Для случая тригонометрических рядов подобный результат получен в работе [2].

Литература:

[1] Б.И.Голубов, А.В.Ефимов, В.А.Скворцов, Ряды и преобразования Уолша: теория и применения, Москва «Наука», 1987 г.

[2] F. Moicz and A. Veres, On the absolute convergense of multiple Furier series, Acta Math. Hungar. 117(2007), 275-292.

УДК 681.3.05

АҚПАРАТ АЛМАСУ ХАТТАМАЛАРЫНДА ҚОЛДАНЫЛАТЫН КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРДІҢ КЕЙБІРІН САЛЫСТЫРУ

Бейбітхан Е.

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің магистранты, Астана

Ғылыми жетекші: ШАРИПБАЕВ А.А., т.ғ.д. профессор

Ақпарат алмасу хаттамалары дегеніміз – барлық абоненттерге алдын–ала белгілі реглементтік тізбекті хабарламаны жіберумен сәйкес абонеттердің өзара әрекеттесуі. Хабарламаны өңдеу және дайындау үшін ақпарат алмасу хаттамаларының жол шеңберінде абоненттер деректерді өңдеудің әр түрлі криптографиялық технологияларын қолданады.

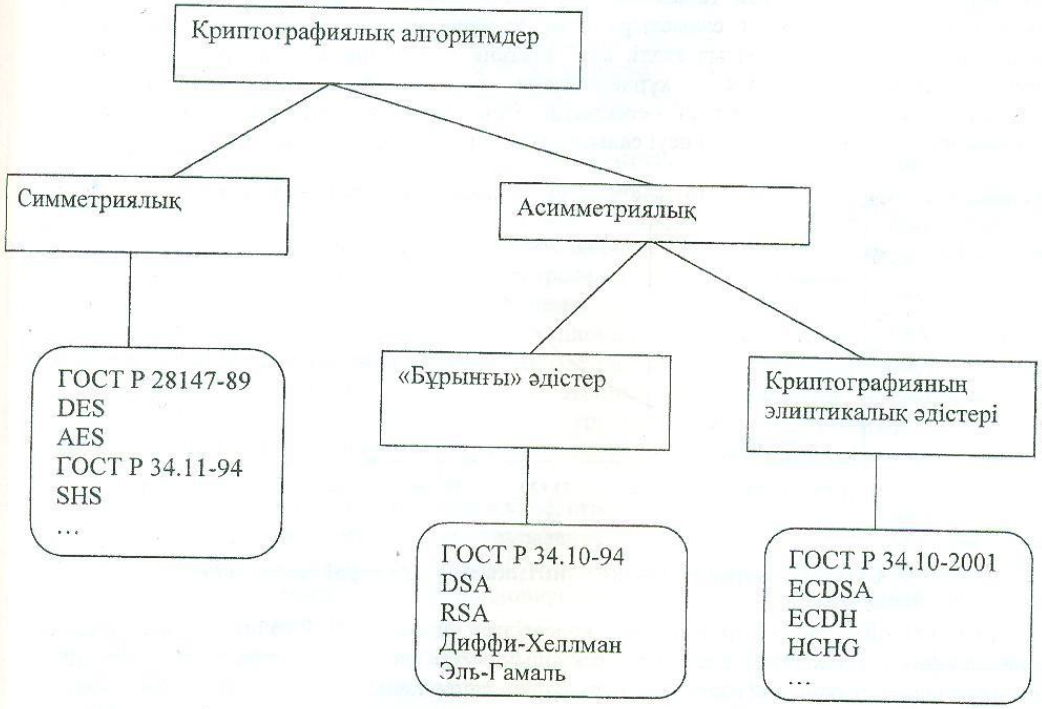
Қолданылатын алгоритмдердің екі типі бар: симметриялық және асимметриялық. Симметриялық деп бір ғана кілт қолданылатын алгоритмді айтады. Ашық кілтті алгоритмдерде әр түрлі кілттер қолданылады. Осы себепті әр түрлі процестерде әр түрлі кілттер қолданылады, ашық кілтті алгоритмді асимметриялық алгоритмдер деп атайды. Симметриялық алгоритмдерді қолданған жағдайда байланыс арнасының екі типі кездеседі. Оның бірі ашық, екіншісі қорғалған болады.

Әр абонент бастапқыда өзінде қос кілтті байланысқан *E* ашық кілтті және құпия *D* кілтін генерирлейді. Ашық кілттерді кейбір сенімді ***кілттерді бөлу орталығында*** жариялайды. Бұл орталық ақыры барлығына ашық кілттердің көшірмелерін береді. Шифрлеу алушының ашық E кілтінде жасалынады. Шифрленген құпиялы D кілтінде оқылады. Қастық ойлаушы адам желідегі әрбір екі абонент арқасында деректер жөнелту каналдарына, сондай-ақ абоненттер арасында және сенімді *кілттерді бөлу орталығында* ене алады. Сызбада құпиялы қорғаулы байланыс каналдары болмайды. *A* қолданушы *B* қолданушыға құпиялы хабар жіберсін. Хабарды шифрлегенде ашық кілтті криптографиялық жүйе қолданылады. *B* қолданушыда өзінің ашық E_n кілті және құпиялы D_n кілті бар. Ашық *EB* кілті барлық қолданушыларға белгілі және жарияланған, сонымен қатар *A* қолданушыға белгілі және ол E_n ашық кілтті хабарды шифрлеу үшін қолданады. *A* қолданушы шифрлеу алгоритмдерін қолданады. Оның негізінде кейбір *F* функциясының екі аргументтері: бастапқы хабар және алушының ашық кілті болады. Функцияның мәні *C* криптограммасы болып табылады. Оны қорғаусыз ашық байланыс каналдары арқылы жіберуге болады. *A* қолданушы $C=F(M, E_n)$ кодтау операциясын орындайды да, *B* қолданушыға криптограмманы жібереді. *B* қолданушы *C* криптограммасын алып, өзінің құпиялы кілті арқылы $M=F(C, D_n)$ дикодтауды орындайды. Нәтижесінде *B* қолданушы құпиялы хабардың бастапқы мәтінін алады.

Криптографиялық алгоритмнің негізінде жатқан сол бір F функциясы арқылы хабарды кодтауға және дикодтауға болады. Жалпы жағдайда әр түрлі функцияларды қолдануға болады.

Қазіргі заманның деректер кодтауы симметриялық криптографиялық алгоритмдер класына жатады. Нақтырақ айтқанда симметриялық блоктық итерациондық кодтау тобына жатады. Бұларға, мысалы, ГОСТ 28147-89, FIPS PUB 46-3 (DES), FIPS PUB 197 (AES) стандарттар жатады. Электронды цифрлы қол стандарты және кілттерді орналастыру ашық кілті криптографиялық алгоритмдер класына жатады. Тәжірибе жүзінде математикалық әдістің екі кластары таратушылық алды. Осы кластар арқылы қазіргі заманғы ашық кілтті криптографиялық жүйелер жасалынады. Бұларға Эль-Гамальдың электронды цифрлы қолдар алгоритмі және Диффи-Хеллманның протоколы жатады және қазіргі заманғы стандартты электронды цифрлы қолдар ГОСТ Р 34, 10-94 және ГОСТ Р 34, 10-2001, хэш алгоритмін қолданылуымен, американдық DSA және ECDSA алгоритмдермен және көптеген криптографиялық протоколдар арқылы ГОСТ Р 34, 11-94 жазылған.

Шифрлеу алушының E кілтінде жасалынады. Шифрлеуді ашып алушының D кілтінде жүзеге асырылады.

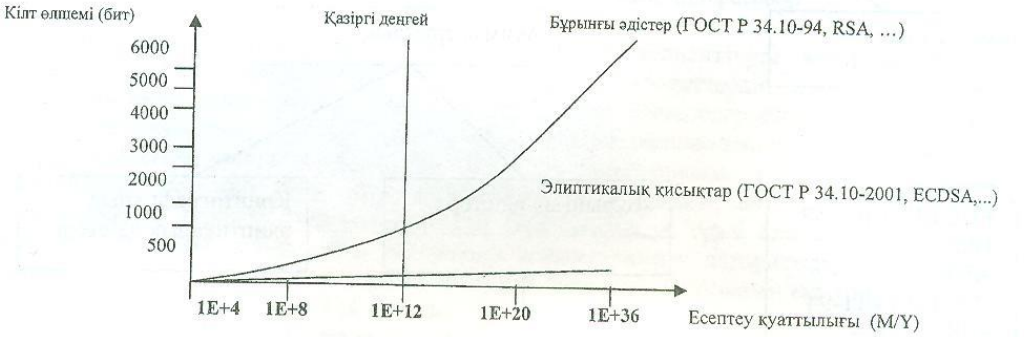


Сурет-1. Криптографиялық алгоритмдер

Егер S жиынында коммутативтік, ассоциативтік, дистрибуттік, тұйық, бірлік және кері элементтері болатын қасиеттерді қанағаттандыратындай қосу, көбейту амалдары анықталған болса, онда S жиынын F өрісі деп атаймыз. Шекті элементі бар өріс **шекті өріс** деп аталады және жалпы жағдайда Fq деп белгіленеді. $q = p^r$, p – жай сан, ал r-бүтін оң сан. Егер r=1 болса, онда өріс қысқалығы Fp мәнін береді. Кей кезде мұндай өрістер Галуа өрістері деп те аталады және $GF(p)$ деп белгіленеді. Есептеу p модулі бойынша модульдік алгебра ережесімен жүзеге асырылады, яғни есептің нәтижесі $[0, p-1]$

интервалында жатады деп есептейміз. Егер p – жай сан болса, онда бұдан шығатыны, кез келген $\alpha \in (0, p-1]$ элементі үшін мультипликатты кері элемент болып табылады. Мұндай элементтердің жиындары [1] мультипликатты топтар құрайды. Қазіргі кездегі ақпарат алмасу хаттамаларында қолданылатын асимметриялы криптографиялық алгоритмдердің көпшілік басым бөлігі экспоненттеу амалдарын қолданады.

Кейбір алгоритмдерде, мысалы, Эль-Гамальдің электронды-цифрлі қолтаңбасының сызбаларында, ГОСТ Р 34.10- 94 стандарттарында, DSA және басқаларда құпия кілт қолтаңбасында [2, 3] модулі бойынша дәрежеге көтеру нәтижесі ретінде қабылданады. Басқа алгоритмдердің, мысалы, RSA сызбасында модуль бойынша r дәрежесіне көтеру нәтижесінің шығуы хабарламаны шифрлеу және дешифрлеу процедураларында қолданылады [4]. Алғашқы жарыққа шыққан Диффи-Хеллманның экспоненттi кілт алмасу асимметриялық алгоритмі жалпы құпия мәнді генерациялау үшін осы амалдарды қолданған еді. $b = a^n \bmod p$ экспоненттеу операциясының кең таралуы шекті өрісте дискреттік логарифмдеу есептері деген атқа ие болған операциясы есепті кері шығару күрделігімен байланысты [6]. a, b және p мәндері белгілі болатын болса, онда n мәнін есептеуі күрделі мәселені шешу есебі болып табылады [7]. Эллиптикалық қисық криптожүйесі бұрын шыққан криптожүйелермен салыстыра отырып кіші мәнді сандарды қолдану кезіндегі беріктілік деңгейін қамтамасыз етеді, ал беріктілік шекті өрістегі дискреттік логарифмде немесе есептің факторлық күрделілігінде қортындыланады. 2-суретте есептеу қуаттылығының өсуіне тәуелді беріктіктің адекваттық деңгейін қамтамасыз ету үшін қолданылған сандар мөлшерінің өсуі салыстырмалы графикте келтірілген.



Сурет-2. Бұрынғы және элиптикалық әдістерді салыстыру

MIPS/YEAR - де келтірілген қуат көрсетілген, яғни M/Y - элиптикалық қисықты криптография қолданылған жағдайда секундына бір миллион операцияны орындайтын компьютердің шыққан жылы. Салыстыру үшін элиптикалық қисықтарда криптографияны қолдану кезінде 160 бит мөлшерлі сандарды, тең алгоритмдерді қолдану кезінде 1024 бит қатардағы сандармен салыстырғандағы эквивалентті тіреуіш деңгеймен қамтамасыз етеді. Келтірілген графиктен көрініп тұрғандай элиптік қисықтарға криптографияларды қолдануға көшу жақын болашақта көрнекті жетістіктер беретіні көрініп тұр.

Әдебиет

1. Акритас А. Основы компьтерной алгебры с приложениями. М.: Мир, 1994.
2. Зима В., Молдовян А., Молдовян Н .Безопасность глобольных сетевых технологий. СПб ;BHV Санкт- Петербург ; 2002
3. Иванов М .А Криптографичские методы защиты информации в компьютерных системах в сетях. М: КУДИЦ – ОБРАЗ, 2001