Қазақстан Республикасының Бірінші Президенті күніне арналған **«Сейфуллин оқулары – 9:** жоғарғы білім және ғылым дамуындағы жаңа бағыт» атты Республикалық ғылыми-теориялық конференция материалдары = Материалы Республиканской научно- теоретической конференции **«Сейфуллинские чтения – 9:** новый вектор развития высшего образования и науки**»** посвященная дню Первого Президента Республики Казахстан. – 2013. – Т.2, ч.1. – Б. 335-336

АҚПАРАТТЫ ҚОРҒАУДЫҢ КРИПТОГРАФИЯЛЫҚ ӘДІСТЕРІ. RSA ЖҮЙЕСІ

Сыздықова З.М.

Ақпараттық технологияның қарқынды дамуы және Интернеттің кеңінен қолданылуы ақпаратты қорғау әдістерін дамытуға көп әсер етті. Қазіргі кездегі ақпараттық технологиялардың дамуы компьютерлік қылмыстар және солармен байланысты ақпараттың ұрлануының өсуімен қосарланып отыр.

Ақпараттың қорғалуын қамтамасыз ету үшін біріншіден, туындаған проблеманың қаншалықты маңызды екенін білу керек, екіншіден, оны шешудің негізгі жолдары мен әдістерін бөліп алу қажет. Ақпаратты қорғау негізінде тек компьютерлік ақпарат емес, және басқа да көптеген аспектілер: фирманың бухгалтерлік есебі, шоттағы ақшаның саны, іспеттес серіктестер, келіссөздер мен жасалған келісімдер және тағы да басқалар жататынын есте сақтаған жөн.

Ақпаратты қорғау ақпараттың сапалы сақталуын қамтамасыз етеді. Ол ең алдымен келесілерге кепілдік береді: конфиденциалдық; ақпараттың сақталуы мен өзгермеуі; ақпаратты тек қажетті қолданушының ала алуы.

Соңғы жылдардағы компьютердің барлық шығармашылық түрлеріне кең енуі, олардың есептеу қуатының ылғи өсуі, әр түрлі масштабтағы компьютерлік желілерді қолдану, берілгендерді өңдеу жүйесіндегі конфиденциалды мәліметтердің жоғалу қаупі компьютерлік әлемнің айырылмас бөлігі болуына әкеліп соқты.

Ақпаратты қорғау объектісі ретінде компьютерлік жүйе немесе берілгендерді өңдеудің автоматтандырылған жүйелерін айтамыз. Автоматтандырылған жүйелерде ақпаратты қорғау жұмыстарын жүргізгенде компьютерлік жүйелер терминімен жиі ауыстырылатын соңғы уақытқа дейін берілгендерді өңдеудің автоматтандырылған жүйелерінің термині қолданылады.

Қазіргі уақытта белгілі кілтпен ақпараттың криптографиялық қорғанысының аса дамыған тәсілі шығарушыларының тектерінің бастапқы әріптерімен аталған (Rivest, Shamir және Adleman) RSA болып табылады. RSA криптожүйесі натурал сандарды жай көбейкіштерге жіктеудің қиындығына негізделген.

RSA алгоритмін қолдану үшін келесі қадамдарды орындай отырып ең алдымен ашық және жасырын кілттерді генерациялау керек:

1. p және q деген екі өте үлкен жай сандарды таңдаймыз.
2. p-ні q-ға көбейтудің нәтижесін n деп анықтаймыз (n=p*q).
3. d деп атайтын үлкен кездейсоқ санды таңдайық. Бұл сан көбейтіндінің санымен өзара жай болуы керек (p-1)*(q-1).

4. Келесі қатынасты қанағаттандыратын e санын анықтаймыз:

(e*d) mod ((p-1)*(q-1))=1.

5. Ашық кілт деп e және n сандарын, ал жасырын кілт деп d және n сандары аталады.

Енді мәліметтерді белгілі кілттермен {e, n} шифрлеу үшін келесі амалдарды орындау қажет:

- шифрленетін мәтінді әрқайсысы M(i)=0, 1,..., n-1 санының түрінде берілетін блоктарға бөлу;
- M(i) сандарының тізбегі ретінде қарастырылатын мәтінді мына формула бойынша шифрлеу: C(i)=(M(i)^e) mod n.

Бұл мәліметтерді {d,n} жасырын кілтін қолдана отырып кері шифрлеу үшін келесі есептеулерді орындау қажет: M(i)=(C(i)^d) mod n. Нәтижесінде өз бойында негізгі мәтінді білдіретін M(i) көптеген сандары алынады.

P (оны дұрыс таңдағанда) жай санының екілік жазбасының ұзындығына байланысты дискреттік логарифмдеу есептерінің күрделілігін бағалау кестеде көрсетілген:

Кесте 1 – Дискреттік логарифмдеу есептерінің күрделілігі

P ұзындығы (биттермен)	x кілтін анықтаудың күрделілігі	Алгоритмнің пайдаланатын жадысы (биттермен)	10^9 оп/с түріндегі компьютерде есепті шығару уақыты
128	$2*10^{12}$	$7*10^6$	Бірнеше минут
200	10^{16}	10^8	Бірнеше ай
256	$9*10^{17}$	10^9	Бірнеше онжылдық
512	$4*10^{24}$	$3*10^{12}$	100 жылға жуық үздіксіз жұмыс
1024	10^{34}	10^{17}	
1500	10^{41}	$8*10^{20}$	
2000	$7*10^{47}$	10^{24}	
2200	10^{50}	10^{25}	

Барлық ассимметриялық криптожүйелерді кілттерді тікелей іріктеп алу жолымен бұзуға тырысады. Сондықтан ассимметриялық криптожүйелерде ұзын кілттерді пайдаланады. Қорғаныстың баламалы деңгейін қамтамасыз ету үшін ассимметриялық криптожүйенің кілті симметриялық криптожүйенің кілтінен анағұрлым ұзын болуы керек. Бұл шифрлеу үшін қажет есептеуіш қорларға әсер етеді. Брюс Шнейер «Қолданбалы криптография: протоколдар, алгоритмдер және С-дағы негізгі мәтін» деген кітапта кілттердің баламалы ұзындықтары туралы келесі мәліметтерді келтіреді.

Кесте 2 - Кілттердің баламалы ұзындықтары

Симметриялық кілттің ұзындығы (биттермен)	Ашық кілттің ұзындығы (биттермен)
56	384
64	512
80	768
112	1792
128	2304

Ассимметриялық шифрлеудің алгоритмдерінің төмен жылдамдығын болдырмау үшін әрбір хабарлама үшін уақытша симметриялық кілт

генерацияланады және тек сол ғана ассимметриялық кілттермен шифрленеді. Хабарламаның өзі осы уақытша сеанстық кілттің көмегімен шифрленеді. Одан кейін осы сеанстық кілт алушының ашық ассимметриялық кілтінің және шифрлеудің ассимметриялық алгоритмінің көмегімен шифрленеді. Бұдан кейін бұл шифрленген сеанстық кілт шифрленген хабарламамен бірге алушыға беріледі. Алушы шифрлеудің сол ассимметриялық алгоритмін және сеанстық кілтті қайта шифрлендіру үшін өзінің құпия кілтін пайдаланады, ал алынған сеанстық кілт хабарламаның өзін қайта шифрлеу үшін пайдаланылады.

Бұл мәселенің өзектілігі жылдан жылға көптеген ақпаратты өңдеуді қажет ететін үлкен есептер ағынымен, олардың программалық және аппаратуралық шешімімен байланысты болып отыр. Мұндай есептерді шешудің бірден-бір жолы – криптографиялық әдістерді, оның ішінде RSA жүйесін қолдану. Осы әдісті қолдану әр-түрлі салаларда конфиденциалды ақпаратты қорғаудың тиімді жүйесін құрайды.

Ғылыми жетекші А.Г.Шаушенова