ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

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
ББК 72+74

ISBN 978-601-337-871-8

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2023

Таким образом, в отличие от шифрсистем PRINT-48 и PRINT-96, шифрсистема GPRINT использует произвольные s-бокс, подстановки σ, $\bar{\rho}_k$ и длину n блока открытого текста.

Пусть $a(u) = \left(a_{\delta\varepsilon}(u)\right)$ — разностная матрица подстановки $u \in S(V_m)$,, т.е.

$$a_{\delta\varepsilon}(u) = 2^{-m}|\{\beta \in V_m|\ (\beta \oplus \delta)^u \oplus \beta^u = \varepsilon\}|,$$

где $\delta, \varepsilon \in V_m$.

Список использованных источников

1. Knudsen L., Leander G., Poschmann A., Robshaw M. J. B. PRINTcipher: A block cipher for ICPrinting // CHES-2010. — Lect. Notes Comput. Sci., 2010. — V. 6225. — P. 16–32.
2. Bogdanov A., Knudsen L. R., Leander G., Paar C., Poschmann A., Robshaw M. J. B., Seurin Y., Vikkelsoe C. PRESENT - An ultra-lightweight block cipher. // CHES 2007. — Lect. Notes Comput. Sci., 2007. — V. 4727. — P. 450–466.

ӘОЖ 004.056.5

ҚОРҒАНЫС ТҮРЛЕНДІРУЛЕРІНІҢ АЛГЕБРАЛЫҚ АЛГОРИТМДЕРІ

Ануарбеков Алмас Маратович
anuarbekovalmas7@gmail.com
Л.Н.Гумилев атындағы ЕҰУ механика-математика факультетінің криптология мамандығының 1-курс магистранты
Ғылыми жетекшісі – Қозыбаев Д.Х.

Қазіргі әлемде ақпарат қауіпсіздігі өте маңызды рөл атқарады. Хабарлар тасымалданатын байланыс арналары көбінесе қорғалмаған болып келеді және осы арнаға қатынас құру құқығы бар кез келген адам хабарларды қолға түсіре алады. Сондықтан тораптарда ақпаратқа біраз шабуылдар жасау мүмкіндігі бар. Бұзушы - тиым салынған операцияларды қателескендіктен, білместіктен орындауға әрекет жасаған немесе ол үшін саналы түрде әртүрлі мүмкіншіліктерді, әдістерді және құралдарды қолданатын тұлға. Ақпаратты қорғау құралдары- мемлекеттік құпия болып табылатын мәліметтерді қорғауға арналған техникалық, криптографиялық, бағдарламалық және басқа да құралдар, олар жүзеге асырылған құралдар, сондайақпарат қорғаудың тиімділігін бақылау құралдары.

Ақпаратты қорғауды қамтамасыз етудің маңызды механизмдерінің бірі ақпаратты түрлендіру болып табылады. Ақпаратты қорғау алгоритмдерін оңтайландыру мәселелері компьютерлік желілердегі ақпарат ағындарының ұлғаюына әкелетін жад құрылғыларының көлемінің және процессор өнімділігінің жылдам өсуімен сипатталатын қазіргі заманғы компьютерлік техниканың дамуының тұрақты тенденцияларына байланысты маңыздырақ болып отыр. Трансформация алгоритмдерінің ең маңызды параметрлері түрлендірудің тұрақтылығы мен жылдамдығы болып табылады. Қауіпсіздіктің осы деңгейінде ақпаратты қорғау алгоритмдерінің жылдамдығының артуы, әсіресе автоматтандырылған басқару жүйелерінің ішінде бөлінген есептеу желілерінің жұмысын айтарлықтай жақсартуға мүмкіндік береді.

Бұл мәселеге ең математикалық қатал тәсіл криптология шеңберінде. Шеннонның классикалық жұмысына сәйкес оқиғаның ықтималдығы криптограмманың ашу қабілеттілігінің өлшемі ретінде пайдаланылады: «белгілі криптограмманы ескере отырып, ашық мәтіннің таңдалған бағасы шынайы ашық мәтінмен сәйкес келді». Бірақ бұл

жағдайда қатаң ықтималдық кеңістігі анықталмаған, оның элементі криптожүйелердің қауіпсіздігінің мәнді бағалауларын алудың біркелкі процедурасын құруға мүмкіндік бермейтін оқиға болып табылады. Осылайша, бүгінгі күні белгілі әдістермен алынған белгілі бір криптожүйенің беріктігін кез келген бағалау оны ашудың белгіліге қарағанда жылдам жұмыс істейтін жаңа әдісінің (алгоритмінің) болмайтынына кепілдік бермейді. Құпия кілті бар криптожүйелердің қауіпсіздігін бағалауды алудың қолданыстағы әдістері негізінен Шеннон идеяларының дамуы болып табылады және эмпирикалық сипатқа ие. Сонымен қатар, криптоаналитиктің оның шексіз есептеу және уақыт ресурстары болуы мүмкіндігіне қатысты болжамдарды жиі жасау қажет.

Ақпараттық қауіпсіздік алгоритмдерін оңтайландыру мәселелері басты мәнге ие. Ақпаратты түрлендірудің жоғары жылдамдықты алгоритмдерін кеңінен қолдану олардың тұрақтылығын бағалауды талап етеді. Бұл ретте қарсылық шабуылдардың нақты түрлеріне қатысты бағаланады. Қолданылатын жүйелердің сенімділігін негіздеу әртүрлі типтегі шабуылдарды модельдеу арқылы эксперименталды түрде жүзеге асырылады. Бұл жағдайда, әдетте, практикаға қарағанда тұрақтылықты талдауда қолайлы жағдайлар қарастырылған. Алгоритм осы шарттарда сенімді болса, оны нақты қолданба үшін ұсынылады.

Ақпаратты қорғаудың криптографиялық алгоритмдері ақпараттың құпиялылығы мен тұтастығын қамтамасыз ету үшін қажет. Бұл есепте біз қорғаныс түрлендірулерінің алгебралық алгоритмдерін және олардың ақпаратты қорғаудағы рөлін қарастырамыз. Қорғаныс түрлендірулерінің алгебралық алгоритмдері ақпараттың қауіпсіздігін қамтамасыз етеді. Криптографиялық алгоритмдер ақпаратты қорғаудың заманауи технологияларының ажырамас бөлігі болып табылады. Қорғаныс түрлендірулерінің алгебралық алгоритмдері-бұл математикалық функцияларды қолдана отырып, деректерді түрлендіру арқылы ақпараттың құпиялылығын, тұтастығын және қол жетімділігін қамтамасыз ететін математикалық процестер. Алгебралық алгоритмдер криптографиялық алгоритмдердің бір түрі болып табылады және ақпаратты шифрлау және дешифрлау үшін қолданылады.

Қорғаныс түрлендіру алгоритмдері-бұл математикалық функцияларды қолдана отырып, деректерді түрлендіру арқылы ақпараттың құпиялылығын, тұтастығын және қол жетімділігін қамтамасыз ететін математикалық процестер. Криптографиялық алгоритмдерді екі топқа бөлуге болады: симметриялы және асимметриялық. Симметриялық алгоритмдер деректерді шифрлау және шифрын ашу үшін бірдей кілтті пайдаланады, ал асимметриялық алгоритмдер цифрлық құжаттарды шифрлау және қол қою үшін ашық және жеке кілттерді пайдаланады.

Асимметриялық алгоритмнің мысалы-RSA. RSA – бұл алгоритмді жасаушылардың фамилияларын білдіретін аббревиатура-Ривест, Шамир және Адлеман. RSA сандық құжаттарды шифрлау және қол қою үшін қолданылады. Ол сандар теориясы мен топтар теориясының математикалық принциптеріне негізделген. RSA-ның негізгі қағидасы - үлкен жай сандарды факторизациялаудың күрделілігі оны шабуыл үшін жарамсыз етеді. RSA ақпаратты қорғаудың ең танымал алгоритмдерінің бірі болып табылады және SSL, TLS және SSH сияқты интернет протоколдарында кеңінен қолданылады.

Симметриялық алгоритмнің мысалы-AES. AES-Advanced Encryption Standard үшін аббревиатура. AES деректерді шифрлау және шифрын ашу үшін қолданылады. Оны ұлттық стандарттар және технологиялар институты (NIST) әзірледі және ақпаратты қорғаудың ең сенімді алгоритмдерінің бірі болып табылады. Ол 128 биттік блоктық шифрлауды қолданады және 128, 192 немесе 256 биттік кілттерді қолдана алады.

Симметриялық алгоритмнің тағы бір мысалы-Blowfish. Blowfish деректерді шифрлау және шифрын ашу үшін қолданылады және ұзындығы 32-ден 448 битке дейінгі кілттерді қолдана алады. Ол сондай-ақ блок өлшемі 64 бит болатын блоктық шифрлауды пайдаланады.

Қорғаныс түрлендірулерінің алгебралық алгоритмдерінің басты артықшылықтарының бірі-олар дұрыс іске асырылған кезде қауіпсіздіктің жоғары деңгейіне ие. Сонымен қатар, алгоритмдерді аппараттық құралдармен жеделдетуге болады, бұл үлкен көлемдегі деректерді жылдам өңдеуге мүмкіндік береді. Бұл алгоритмдердің барлығы ақпаратты шифрлау және шифрын ашу үшін үлкен санды операциялар, Галуа түрлендірулері, XOR операциялары және т.б. сияқты математикалық функцияларды пайдаланады. Олар деректерді тек кілті бар адам ғана деректердің шифрын ашып, ақпаратқа қол жеткізе алатындай етіп түрлендіру арқылы ақпаратты қорғауды қамтамасыз етеді.

Қорғаныс түрлендіру алгоритмдерінің беріктігін оларды бұзу үшін қолдануға болатын шабуылдар арқылы бағалауға болады. Ең көп таралған шабуылдардың бірі-шабуылдаушы дұрыс комбинацияны тапқанға дейін барлық мүмкін кілттер тіркесімін немесе басқа алгоритм параметрлерін сұрыптайтын шамадан тыс шабуыл.

Мұндай шабуылдарға қорғаныс түрлендіру алгоритмдерінің беріктігін арттыру үшін S-блоктары, элементтерді ауыстыру, бағандарды араластыру және жолдарды ауыстыру сияқты қосымша түрлендірулер жиі қолданылады. Алайда, түрлендірулердің тіркесіміне негізделген алгоритмдерді түсіну қиын болуы мүмкін және оларды шамадан тыс шабуылдармен бұзуға болады.

Алайда, ақпаратты қорғау алгоритмдерін іске асыру кезінде бірқатар шектеулерді ескеру қажет. Біріншіден, қауіпсіздікті қамтамасыз ету үшін кілттер мен алгоритмдерді дұрыс таңдау керек. Екіншіден, кілттерді сақтау және беру қауіпсіздігін қамтамасыз ету қажет. Үшіншіден, мүмкін шабуылдарды қиындату үшін жеткілікті күрделі алгоритмдер мен кілттерді қолдану қажет.

Қорыта айтқанда қорғаныс түрлендірулерінің алгебралық алгоритмдері ақпараттың қауіпсіздігін қамтамасыз етуде маңызды рөл атқарады. Олар цифрлық құжаттарды шифрлау және қол қою, деректердің құпиялылығы мен тұтастығын қамтамасыз ету үшін қолданылады. Мұндай алгоритмдердің мысалдары RSA, AES және Blowfish болып табылады. Алайда, ақпаратты қорғау алгоритмдерін іске асыру кезінде бірқатар шектеулерді ескеру және деректердің қауіпсіздігін қамтамасыз ету үшін дұрыс тәжірибелерді сақтау қажет.

Қолданылған әдебиеттер тізімі:

1. Иванов М. А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях.- М.: НИЯУ МИФИ, 2012.

2. Молдовян Д.Н., Молдовян Н.А. Введение в теоретические основы криптоситем с открытым ключом.-- СПб.: Изд–во ГУМРФ им. адмирала С.О. Макарова, 2016.

3. Лось А.Б., Нестеренко А.Ю., Рожков М.И. Криптографические методы защиты информации. –М.: Юрайт, 2016.

ӘОЖ 004.056

АШЫҚ КІЛТТІ КРИПТОГРАФИЯЛЫҚ ЖҮЙЕГЕ НЕЙРОНДЫҚ ЖЕЛІЛЕРДІҢ ҚОЛДАНЫЛУЫ

Асқарқызы Нұргүл

askarkyzyng@gmail.com

Л.Н.Гумилев атындағы ЕҰУ «6В06105- Математикалық және компьютерлік модельдеу» мамандығының 4 курс студенті, Астана, Қазақстан

Ғылыми жетекшісі- К.М. Сулейменов