ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

А.БАЙТҰРСЫНОВ АТЫНДАҒЫ ҚОСТАНАЙ ӨҢІРЛІК УНИВЕРСИТЕТІ

СҰЛТАНҒАЗИН ОҚУЛАРЫ

«ҚАЗІРГІ БІЛІМ БЕРУДІ ДАМЫТУДЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ»
ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ-ПРАКТИКАЛЫҚ КОНФЕРЕНЦИЯ

МАТЕРИАЛДАРЫ

СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ

МАТЕРИАЛЫ

МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
«АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ СОВРЕМЕННОГО ОБРАЗОВАНИЯ»

Қостанай, 2023

УДК 378 (094)
ББК 74.58
Қ 22

РЕДАКЦИЯ АЛҚАСЫ/ РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Куанышбаев Сеитбек Бекенович, А.Байтұрсынов атындағы Қостанай өңірлік университетінің Басқарма Төрағасы – Ректоры, география ғылымдарының докторы, Қазақстан Педагогикалық Ғылымдар Академиясының мүшесі; / Председатель Правления – Ректор Костанайского регионального университета имени А.Байтурсынова, доктор географических наук, член Академии Педагогических Наук Казахстана;

Жарлыгасов Женис Бахытбекович, А.Байтұрсынов атындағы Қостанай өңірлік университетінің Зерттеулер, инновация және цифрландыру жөніндегі проректоры, ауыл шаруашылығы ғылымдарының кандидаты, қауымдастырылған профессор / проректор по исследованиям, инновациям и цифровизации Костанайского регионального университета им. А.Байтурсынова, кандидат сельскохозяйственных наук, ассоциированный профессор;

Хуснутдинова Ляйля Гельсовна, тарих ғылымдарының кандидаты, «Мәскеу политехникалық университеті» Федералды мемлекеттік автономды жоғары білім беру мекемесінің доценті, Ресей / кандидат исторических наук, доцент Федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет», Россия;

Сухов Михаил Васильевич, техника ғылымдарының кандидаты, Оңтүстік- Орал мемлекеттік университетінің (ООМУ) доценті, Челябі, Ресей/кандидат технических наук, доцент Южно-Уральского государственного университета (ЮУрГУ), г. Челябинск, Россия;

Радченко Татьяна Александровна, жаратылыстану ғылымдарының магистрі, А.Байтұрсынов атындағы Қостанай өңірлік университетінің «Физика, математика және цифрлық технологиялар» кафедрасының меңгерушісі / магистр естественных наук, заведующая кафедрой «Физики, математики и цифровых технологий» Костанайского регионального университета им. А.Байтурсынова;

Алимбаев Алибек Алпысбаевич, PhD докторы, А.Байтұрсынов атындағы Қостанай өңірлік университетінің «Физика, математика және цифрлық технологиялар» кафедрасының қауымдастырылған профессорының м.а. / доктор PhD, и.о.ассоциированного профессора кафедры «Физики, математики и цифровых технологий» Костанайского регионального университета им. А.Байтурсынова;

Телегина Оксана Станиславовна, А.Байтұрсынов атындағы Қостанай өңірлік университетінің «Физика, математика және цифрлық технологиялар» кафедрасының аға оқытушысы / старший преподаватель кафедры «Физики, математики и цифровых технологий» Костанайского регионального университета им. А.Байтурсынова;

Шумейко Татьяна Степановна, педагогика ғылымдарының кандидаты, А.Байтұрсынов атындағы Қостанай өңірлік университетінің «Физика, математика және цифрлық технологиялар» кафедра профессорының м.а. / кандидат педагогических наук, и.о. профессора кафедры «Физики, математики и цифровых технологий» Костанайского регионального университета им. А.Байтурсынова

Қ 22

«Қазіргі білім беруді дамытудың өзекті мәселелері»: «СҰЛТАНҒАЗИН ОҚУЛАРЫ-2023» Халықаралық ғылыми-тәжірибелік конференцияның материалдары, 2023 жылдың 15 наурызы. Қостанай: А.Байтұрсынов атындағы Қостанай өңірлік университеті, 2023. – 427 б.
«Актуальные вопросы развития современного образования»: Материалы международной научно-практической конференции «СУЛТАНГАЗИНСКИЕ ЧТЕНИЯ-2023», 15 марта 2023 года. Костанай: Костанайский региональный университет имени А.Байтурсынова, 2023. – 427 с.

ISBN 978-601-356-257-5

«Сұлтанғазин оқулары-2023» халықаралық ғылыми-тәжірибелік конференциясының «Заманауи білім беруді дамытудың өзекті мәселелері» жинағында жаратылыстану-ғылыми білім берудің мәселелері мен болашағына арналған ғылыми мақалалар жинақталған, жалпы және кәсіптік білім берудің психологиялық-педагогикалық аспектілері қарастырылған, педагогикалық білім берудің ақпараттандыру және дамытудың қазіргі тенденциялары мен технологиялары мәселелері қозғалады.

Осы жинақтың материалдары ғалымдар мен жоғары оқу орындарының оқытушыларына, магистранттар мен студенттерге пайдалы болуы мүмкін.

В сборнике Международной научно-практической конференции «Султангазинские чтения-2023» «Актуальные вопросы развития современного образования»: представлены научные статьи по проблемам и перспективам естественно-научного образования, рассматриваются психолого-педагогические аспекты общего и профессионального образования, затронуты вопросы информатизации и современных тенденций и технологий развития педагогического образования.

Материалы данного сборника могут быть интересны ученым, преподавателям высших учебных заведений, магистрантам и студентам.

ISBN 978-601-356-257-5
9 786013 562575

УДК 378 (094)
ББК 74.58

© А.Байтұрсынов атындағы Қостанай өңірлік университеті, 2023
© Костанайский региональный университет имени А.Байтурсынова, 2023

Сурет 1 – LDD бағдарламасында жасалған жұмыстар

Сонымен, бұл бағдарлама білім алушылардың, студенттердің білім беру қызметі барысында алған білімдері мен дағдыларын толықтырады және тереңдетеді. Лего дизайны білім алушыларға, студенттерге өз идеяларын жүзеге асыруға, ынта-жігермен жұмыс істеуге және түпкілікті нәтижені көруге, құруға және қиялдауға көмектеседі. Шығармашылық және техникалық мәселелерді шешуде білім алушы талдау, жалпылау, кеңістіктік қиялды дамыту, шығармашылық әлеуетті жүзеге асыру қабілетін қалыптастырады. Бұл бағдарлама робот техниктер үшін ғана емес, болашақ сәулетшілер, мүсіншілер, дизайнерлер үшін де негіз болып табылады.

Әдебиеттер тізімі:

1. Балтабек, Ерлан Ермекулы. Педагогические условия организации элективного курса «Образовательная робототехника» в общеобразовательной школе / Ерлан Ермекулы Балтабек. — Текст : непосредственный // Молодой ученый. — 2022. — № 22 (417). — С. 10-13.
2. LEGO Digital Designer 4.3.8 (Виртуальный конструктор Лего). http://www.lego-le.ru/mir-lego/programmi-lego/legodigital-designer.html

УДК 004.056.2

БЛОКТЫҢ АЙНЫМАЛЫ ФРАГМЕНТАЦИЯСЫ БАР АЛГОРИТМНІҢ ШИФРЛАУ ПАРАМЕТРЛЕРІН ЗЕРТТЕУ

Аманкелді Әсел Жұмағалиқызы, магистрант Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан, E-mail: Amangeldievaaselya161@gmail.com

Кудубаева Сауле Альжановна, техника ғылымдарының кандидаты, Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан, E-mail: saule.kudubayeva@gmail.com

Аңдатпа

Бұл мақалада әртүрлі шифрлау параметрлері (p және q) бар алгоритмнің нәтижелерін зерттеу негізінде әзірленген блоктың ауыспалы фрагментациясы бар шифрлау алгоритмінің параметрлерін таңдау бойынша ұсыныстар берілген. Әр түрлі параметрлерді таңдау кезінде блоктың ауыспалы фрагментациясы бар алгоритмнің нәтижелерін зерттеу екілік көріністегі әртүрлі параметрлерді қолдана отырып, шифрланған тізбектерге статистикалық және графикалық сынақтарды қамтитын жалған кездейсоқ тізбекті тестілеу әдістерін қолдану арқылы жүзеге асырылады. Статистикалық тест

Д. Кнут тесттерінің жиынтығынан таңдалды, атап айтқанда корреляцияны тексеру. Графикалық тестілеу ретінде k-грамм үлестірімінің құрылысы жүргізілді. Жұмыста алгоритмнің әртүрлі шифрлау параметрлері (p және q) жұмысын зерттеу нәтижелері негізінде параметрлерді таңдау бойынша келесі ұсыныстар жасалады: p және q – өзара жай сандар, p-ішкі блоктарға тізбекті бөлу q-ішкі блоктарға (p > q) бөлінуден үлкен.

Түйінді сөздер: шифрлау, шифрлау алгоритмі, жалған кездейсоқ тізбекті тестілеу, статикалық тесттер, графикалық тесттер.

Аннотация

В данной статье представлены рекомендации по подбору параметров алгоритма шифрования с переменной фрагментацией блока, разработанные на основе исследования полученных результатов работы алгоритма с различными параметрами шифрования (p и q). Исследование результатов работы алгоритма с переменной фрагментацией блока при выборе различных параметров проводится с использованием методик тестирования псевдослучайных последовательностей, включающих в себя статистические и графические тесты над шифрованными последовательностями с использованием различных параметров в бинарном представлении. Статистический тест выбран из подборки тестов Д. Кнут, а именно проверка корреляции. В качестве графифического тестирования проводилось построение k-граммного распределения. На основе результатов исследования работы алгоритма с различными параметрами шифрования (p и q), сформулированы следующие рекомендации по подбору параметров: p и q – взаимно-простые числа, разбиение последовательности на p-подблоки больше, чем разбиение на q-подблоки (p > q).

Ключевые слова: шифрование, алгоритм шифрования, тестирование псевдослучайных последовательностей, параметры шифрования, статические тесты, графические тесты.

Abstract

This article presents recommendations for the selection of encryption algorithm parameters with variable block fragmentation, developed based on the study of the results of the algorithm with different encryption parameters (p and q). The study of the results of the algorithm with variable block fragmentation when selecting various parameters is carried out using pseudorandom sequence testing techniques, including statistical and graphical tests on encrypted sequences using various parameters in binary representation. The statistical test is selected from a selection of tests by D. Knuth, namely the correlation test. A k-gram distribution was constructed as graphographic testing. Based on the results of the study of the algorithm with different encryption parameters (p and q), the following recommendations for the selection of parameters are formulated: p and q are mutually prime numbers, splitting the sequence into p–subblocks is greater than splitting into q-subblocks (p > q).

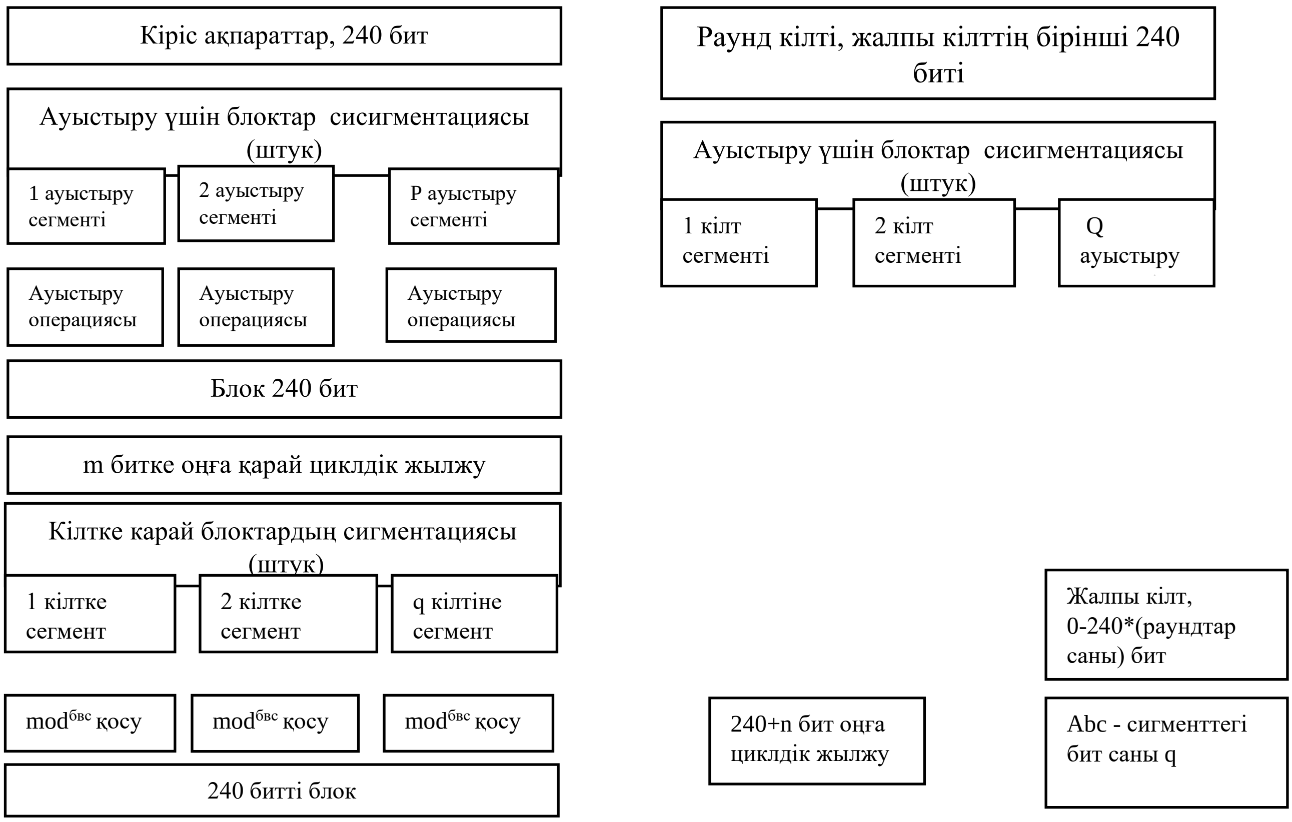
Keywords: encryption, encryption algorithm, pseudorandom sequence testing, encryption parameters, static tests, graphical tests.

Өздеріңіз білетіндей, қазіргі уақытта криптоанализ әдістері белсенді дамуда және сонымен бірге компьютерлік техниканың жылдамдығы артып келеді. Бұл ақпаратты Ашық арналар арқылы беру кезінде шифрлау әдістерін одан әрі жетілдіруді қажет етеді [1].

Бұрын әртүрлі раундтарда [2] криптографиялық қарабайырлардың өлшемдерінің динамикалық өзгеруімен шифрлау алгоритмі ұсынылған, жұмыста [3] осы алгоритмнің модернизациясы ұсынылды, алгоритмнің толық сипаттамасы жұмыста берілген [2], 1-суретте осы алгоритммен шифрлау схемасы көрсетілген.

Жұмыстың мақсаты осындай алгоритм бойынша шифрлау нәтижелерін параметрлер мәндерінің әртүрлі жиынтығымен салыстыру және осы алгоритмді тиімді пайдалану үшін ұсыныстар беру.

Алгоритмді зерттеу үшін параметрлер жиынтығын таңдау. Шифрлау параметрлерін таңдау бойынша ұсыныстар жоқ. Параметрлерді зерттеу кезінде 3 мәтінді шифрлау жүргізілді, мәтіннің ұзындығы 240 битке көбейтілуі керек. Мәтін тым қысқа немесе тым ұзын болмауы керек, сондықтан ұзындығы 240×19 = 4560 бит таңдалады. Шифрлау үшін әртүрлі дәрежедегі 240 биттік кілттер қолданылды.



Сурет 1 – Шифрлау сызбасы

Кесте 1 – Параметрлер графигі

№	Айналым	Параметрлер гр.1	Параметрлер гр.2	Параметрлер гр.3	Параметрлер гр.4
1	1 раунд	(p=4, q=8)	(p=8, q=4)	(p=4, q=9)	(p=9, q=4)
2	2 раунд	(p=3, q=12)	(p=25, q=5)	(p=3, q=8)	(p=8, q=3)
3	3 раунд	(p=2, q=6)	(p=12, q=3)	(p=5, q=9)	(p=9, q=5)
4	4 раунд	(p=5, q=10)	(p=6, q=2)	(p=6, q=11)	(p=11, q=6)
5	5 раунд	(p=6, q=12)	(p=12, q=6)	(p=7, q=12)	(p=13, q=7)
6	6 раунд	(p=7, q=14)	(p=14, q=7)	(p=8, q=13)	(p=15, q=8)
7	7 раунд	(p=8, q=16)	(p=8, q=16)	(p=2, q=5)	(p=17, q=8)
8	8 раунд	(p=9, q=18)	(p=18, q=9)	(p=9, q=17)	(p=19, q=9)

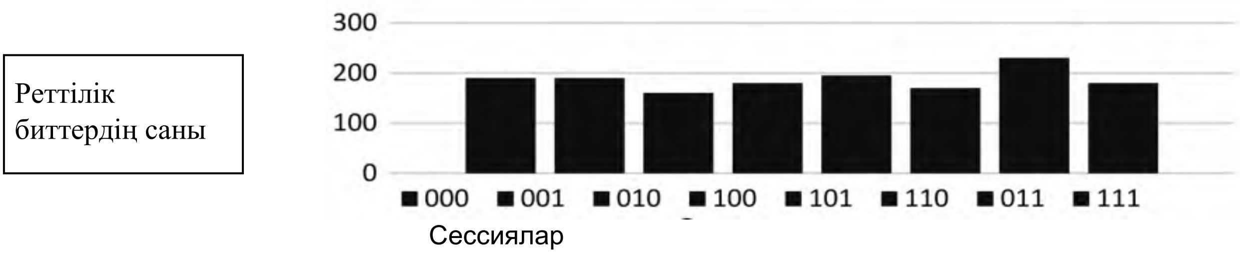
Кілттің тұрақтылығы кілт [4] битінің корреляциясын тексеру нәтижелері бойынша бағаланды, барлығы 7 кілт қолданылды. Ең тұрақты шифрлауды қамтамасыз ететін параметрлерді анықтау үшін кестеде келтірілген параметрлер топтары қолданылды. Шифрлаудың әр раундында алынған шифрланған реттіліктер зерттелді. Әр раундта ауыстыруды әр кіріс және әр шығыс биттері арасындағы нөлдік корреляция коэффициенттері бар кестелерге сәйкес жүргізу ұсынылады. Әр айналымда тиісті мөлшердегі нақты кестені таңдау құпия болып табылады. Барлық параметрлер топтарын келесі сипаттамаларға сәйкес жіктеуге болады:

- өзара қарапайым p және q немесе бірнеше p және q;
- $p > q$ немесе $P < q$.

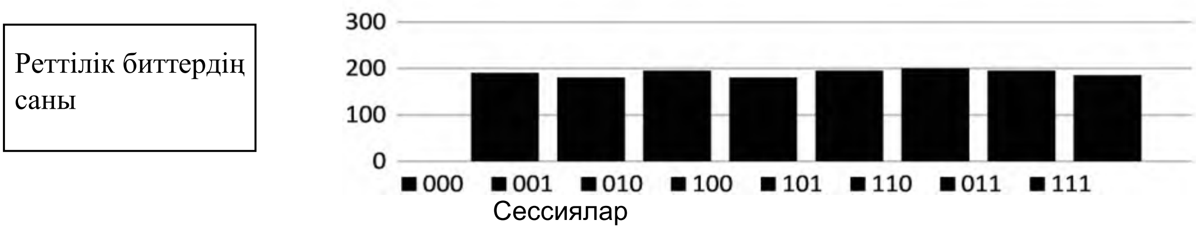
Шифрлау алгоритмінің параметрлерін блоктың ауыспалы фрагментациясымен зерттеу. Блоктың ауыспалы фрагментациясымен алгоритмді шифрлау параметрлерін зерттеу графикалық және статистикалық сынақтардың нәтижелері негізінде жүргізілді. Параметрлердің әр тобын және әрбір кілтін қолдана отырып (кесте 1), шифрлау нәтижесінде алынған әр мәтіннің шифрланған реттілігі тексерілді.

Шифрланған тізбектің сапасын талдау және қасиеттерін өзгерту үшін индикативті тест қолданылды, атап айтқанда k-грам үлестірімі құрылды. Бұл тест k биттерінен тұратын сериялардың пайда болу жиілігін талдау негізінде зерттелген тізбектегі таңбалардың біркелкі таралуын анықтауға мүмкіндік береді. Зерттеуде k = 3 таңдалды, таңбалар сериясының таралуының біркелкілігі анықталды: 000, 001, 010, 100, 110, 011, 111. Қасиеттері кездейсоқ реттілік қасиеттеріне жақын реттілік үшін әр түрдің эпизодтарының пайда болу саны арасындағы шашырау нөлге жетуі керек [5], ашық мәтінде таңбалар сериясының біркелкі таралуы байқалмайды. Осы тестілеуді өткізу үшін шифрлау параметрлерінің әрбір тобы ашық мәтінді шифрлаудың бес раундын өткізді және біркелкі тарату графиктері салынды, толық нәтижелер ұсынылды [4]. 2 суретте екінші параметрлер тобын қолдана отырып, шифрлаудың 5 раундынан кейін серияларды шифрланған ретпен бөлу графигін ұсынады.

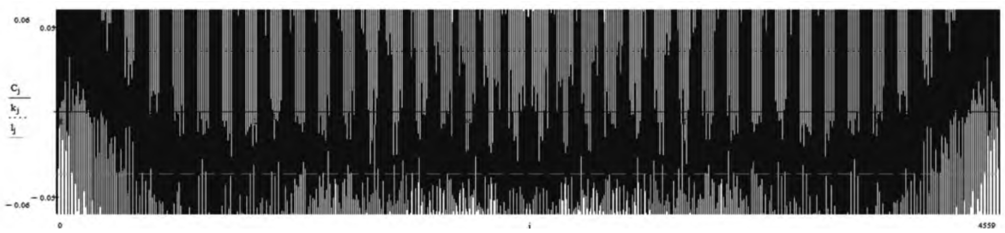
3-суретте көрсетілген шифрлау параметрлерінің (2 сурет) төртінші тобын қолдана отырып, шифрлаудың 5 раундынан кейін, шифрлаудың екінші тобын қолдана отырып, сериялардың таралу графигін шифрланған ретпен салыстырамыз.



Сурет 2 – 5-ші айналымнан кейін екінші параметрлер тобының шифрланған ретпен серияларды таратуы



Сурет 3 – 5-ші раундтан кейін төртінші параметрлер тобымен шифрланған ретпен серияларды бөлу



Сурет 4 – Бастапқы мәтін биттерінің тәуелділік графигі

2-суретте және 3-суретте көрсетілген графиктерге салыстырмалы талдау жасай отырып, төртінші шифрлау тобы алған реттілік қасиеттері кездейсоқ реттілік қасиеттеріне жақын деп қорытынды жасауға болады, бұл шабуылдаушыға ашық мәтінді шифрланған реттіліктен қалпына келтіру қиынға соғады дегенді білдіреді.

Шифрланған тізбектің сапасын талдау үшін Д.Кнуттың таңдауынан статистикалық тест қолданылды. Бұл тест элементтердің өзара тәуелділігін тергеу арқылы тексереді.

$\varepsilon = \varepsilon_1\varepsilon_2 \ldots \varepsilon_n$болсын-ұзындықтың m-биттік сандарының тізбегі N. статистика 1 формула бойынша есептеледі

$$C_j = \frac{n\left(\varepsilon_0\varepsilon_j+\varepsilon_1\varepsilon_{(1+j)} mod\, n^{+\ldots+}\varepsilon_{n-2}\varepsilon_{(n-2+j) mod\, n}+\varepsilon_{n-1}\varepsilon_{(n-1+j) mod\, n}\right)-(\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_{n-1})^2}{n(\varepsilon_0^2+\varepsilon_1^2+\cdots+\varepsilon_{n-1}^2)-(\varepsilon_0+\varepsilon_1+\cdots+\varepsilon_{n-1})^2}. \quad (1)$$

Қандай да бір j мәні C интервалында жатуы керек

$[\mu_n - 2{,}43\sigma_n; \mu_n + 2{,}43\sigma_n]$, бұл жердегі $\sigma^2 = n^2/(n-1)^2(n-2)$[5].(2)

Бұл зерттеуде ұзындығы 4560 биттік екілік тізбекті талдау қолданылады. Тестілеу кезінде есептелген мәндер диапазоны келесі мәндерді қабылдайды: [-0,036224; 0,035786]. Тестілеу нәтижесі график түрінде көрсетіледі (сурет 4) онда есептелетін тестілеу мәндерінің шекаралары көрсетіледі. Графикте диапазон шекаралары үзік-үзік сызықбелгіленеді, одан тыс график шықпауы керек, k_j – диапазонның жоғарғы шекарасы, l_j– диапазонның төменгі шекарасы. Графиктің диапазоннан тыс шығуы шабуылдаушыға ашық мәтінді есептеуге мүмкіндік беретін дәйектілік биттері арасындағы байланыс байқалатынын көрсетеді.

4-суретте бастапқы мәтіндердің бірін тестілеу нәтижелерінің кестесі көрсетілген. 4-суреттегі графикте көрсетілгендей, биттердің ашық бастапқы тізбектегі толық тәуелділігі байқалады. Яғни тесттенөтпеді, шабуылдаушы бастапқы мәтінді бит тізбегінен оңай қалпына келтіре алады.

Бұл мақалада күшті K_2 кілтімен шифрлау кезінде алынған шифрланған тізбектің биттерінің өзара тәуелсіздігін тексеру нәтижесі келтірілген, бұл кілтті тестілеу арқылы дәлелденген [4].
5-суретте параметрлердің төртінші тобын және K_2 кілтін қолдана отырып, шифрлаудың бір раундынан кейін шифрланған реттік биттердің өзара тәуелсіздік графигі көрсетілген, шифрлаудың бір раундын жүргізгеннен кейін күшті кілтпен шифрланған ретті тестілеудің нәтижесі ұсынылған параметрлерді қолдана отырып, сәтті деп санауға болады және осы кезеңде графикте қаралған байланыстар (5 сурет) деп болжауға болады. Параметрлердің төртінші тобын, шифрланған биттер арасындағы байланыстарды пайдалана отырып, шифрлаудың 8 раундын жүргізу кезінде тізбектер байқалмайды [4].

Әр түрлі раундтардағы барлық шифрланған тізбектің тестілеу нәтижелерін салыстыра отырып [4] шифрлау параметрлерінің төртінші тобын қолдану алгоритмнің ең тұрақты нәтижесін береді деп қорытынды жасауға болады. Шифрлау параметрлерінің бірнеше тобын пайдаланған кезде, шифрлау раундтарының аз саны үшін сериялардың шифрланған ретпен біркелкі бөлінуіне қол жеткізіледі. Параметрлердің төртінші тобында P және q таңдалады, бұл p > q және олар өзара қарапайым.

Блоктардың айнымалы фрагментациясы бар симметриялық шифрлау алгоритмінің параметрлерін зерттеу нәтижелері бойынша, бұл алгоритм параметрлерді таңдау кезінде тестілеу нәтижелері жоғары болады деп қорытынды жасауға болады бастапқы бит тізбегінің блоктарын р-блоктарына шифрлау кезінде бөлу бит тізбегін q-қосалқы блоктарға бөлу параметрінен үлкен болды - (p > q), P және q параметрлері өзара қарапайым. Осылайша, айнымалы блок фрагментациясы бар алгоритм үшін шифрлау параметрлерін таңдағанда, р-ішкі блоктарда шифрлау кезінде бастапқы бит тізбегінің блоктарының соғу санын көбейту шифрлау нәтижесін жақсартатынын ескеру қажет деп қорытынды жасауға болады. Айнымалы блок фрагментациясы бар шифрлау алағының алго тестілеу нәтижелерінің жоғары көрсеткіштері бұл алгоритмді деректерді шифрлауды қажет ететін әртүрлі салаларда қолдануға болатындығын көрсетеді.

Әдебиеттер тізімі:

1. Коршиков С. Б., Терентьев М. Н., Мусолов М. Н. Возможности использования метода результативного искажения при создании сложных технических систем в высокотехнологичных отраслях промышленности // Электронный журнал «Труды МАИ». Выпуск № 47.
2. Жданов О. Н., Соколов А. В. Алгоритм шифрования с переменной фрагментаций блока. Проблемы и достижения в науке и технике / Сборник научных трудов по итогам международной научно-практической конференции. № 2. Инновационный центр развития образования и науки – Омск, 2015. – С. 153–159
3. Zhdanov O. N., Sokolov A. V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. / Far East Journal of Electronics and Communications – 2016 Pushpa Publishing House, Allahabad, India – Pages 573–589.
4. Захарова К. О., Методика тестирования алгоритма с переменной фрагментацией блока. [Электронный ресурс] GoogleDrive. URL: https://drive.google.com/open?id=1-RwL2aVF5MHknqnJjYdyAx9CG-MbXB4Q.

5. Иванов, М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.
6. Grosek O., Why use bijective S-boxes in GOST-algorithm. / O. Grosek, K. Nemoga, M. Zanechal // http://www.mat. savba.sk – Slovak Academy of Sciences, Bratislava, 1998, 13 с.
7. Елемесов К. К., Утепова Э. О. О перспективах и возможной области применения криптоалгоритма ЖдановаСоколова. Информационные и телекоммуникационные технологии: образование, наука, практика / Сборник научных трудов по итогам II международной научно-практической конференции. Том II. – Казахстан: Алматы. КазНИТУ имени К. И. Сатпаева, 2015. – С. 110–112.

УДК 004.942

МОДЕЛИРОВАНИЕ КАК ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

Анетова Айжан Жакановна, м.т.н., старший преподаватель, Университет «Туран-Астана», г.Астана, Казахстан, E-mai: Aizhan83@mail.ru
Ерсултанова Зейнеп Сапаргалиевна, старший преподаватель Университет «Туран-Астана», г.Астана, Казахстан, E-mai: ersultanovazs@gmail.com

Аңдатпа

В статье рассматриваются математические модели, используемые в качестве инструмента управления предприятием, анализируется перспективность их применения на практике. Делается вывод об актуальности применения имитационного моделирования как эффективного инструмента управления предприятием.

Ключевые слова: моделирование, математическая модель, управление предприятием, инструмент управления предприятием, эффективность, имитационное моделирование, экономическая система.

Аннотация

Мақалада кәсіпорынды басқару құралы ретінде қолданылатын математикалық модельдер қарастырылады, оларды тәжірибеде қолдану перспективалары талданады. Имитациялық модельдеуді кәсіпорынды басқарудың тиімді құралы ретінде пайдаланудың өзектілігі туралы қорытынды жасалады.

Түйінді сөздер: модельдеу, математикалық модель, кәсіпорынды басқару, кәсіпорынды басқару құралы, тиімділік, имитациялық модельдеу, экономикалық жүйе.

Abstract

The article deals with mathematical models used as a tool for enterprise management, analyzes the prospects of their application in practice. The conclusion is made about the relevance of the use of simulation modeling as an effective tool for enterprise management.

Key words: modeling, mathematical model, enterprise management, enterprise management tool, efficiency, simulation modeling, economic system.

На сегодняшний день применение эффективных инструментов управления предприятием является обязательным условием ведения хозяйственной деятельности.

Сфера применения таких инструментов достаточно широка и охватывает множество предметных областей, таких как: планирование, моделирование бизнес-процессов; прогнозирование; маркетинг; логистика.Инструментально-аналитические подходы так же используют при анализечеловеческого капитала и различных аспектов финансово-хозяйственной деятельности организации, применяют для выявления действенных процедур по стимулированию и мотивации персонала, повышения его производительности, для создания систем автоматизации процессов управления на всех уровнях [1, с.15].

Одним из результативных инструментов управления предприятием, применимым во всех указанных областях, является моделирование явлений ипроцессов, протекающих на предприятии, позволяющее выявить рациональные и наименее затратные способы решения управленческих задач. Зачастую, предприятия функционируют в условиях ограниченного наличия материальных, поэтому необходимо разрабатывать математические модели для изучения показателей, оказывающих влияние на управление хозяйственной деятельностью, учитывающих разносторонние факторы, характеризующие эффективность управления и уровень доходности. В результате моделирования отдельных процессов деятельности предприятия, менеджмент получает актуальную информацию, необходимую для принятия решения. Именно поэтому для повышения эффективности