ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (346)

APRIL – JUNE 2023

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*

Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Тиражы: *300 дана.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Namber 346 (2023). 70–80
https://doi.org/10.32014/2023.2518-1726.185

МРНТИ 81.93.29
УДК 004.056.55

© K. Alibekova[1*], Zh. Alimzhanova[1], S.S. Baizakova[2], 2023

[1]Al Farabi Kazakh National University, Almaty, Kazakhstan;
[2]Arkalyk State Pedagogical Institute named after Y.Alttynsarin, Arkalyk, Kazakhstan.
E-mail: kamalibekova@gmai.com

RATING VALUATION OF BLOCK CIPHERS FOR WIRELESS SENSOR NETWORKS

Alibekova Kamila Nurdauletkyzy — Doctoral student of the Department of Information Systems of the Al-Farabi Kazakh National University, Almaty, Kazakhstan
E-mail: kamalibekova@gmail.com; https://orcid.org/0000-0001-5039-7833;
Alimzhanova Zhanna Muratbekovna — Candidate of Physical and Mathematical Sciences Al-Farabi Kazakh National University, Almaty, Kazakhstan
E-mail: zhannamen@mail.ru, https://orcid.org/0000-0001-6282-5356;
Baizakova Saule Svyazkhanovna — Senior lecturer, Master's degree, Arkalyk State Pedagogical Institute named after I. Altynsarin

Abstract. Security is one of the extensive relations in assorted Wireless Sensor Network (WSN employment. A no of cryptanalytic rules area been developed to acknowledge safe keeping utility in WSNs. However, in an energy-efficient and jackanapes nonbeing is a difficult engagement due care to imagination restricted disposition of device excrescences. Systematic exploration of cryptanalytic rules is, accordingly, requisite to acknowledge an admirable sympathetic of the trade-off between safekeeping about and operation charge. In this idea, we've contemplated cardinal shaft nonentities: Skipjack, Corrected Obstruct Tiny Encryption Algorithm (XXTEA, RC5, Advanced Encryption Standard (AES, and Chaotic-Map and Genetic-Operations supported Encryption Algorithm (CGEA. The about of these ciphers is assessed on Arduino Pro and Mica2 device particles. Then the memory practice, operation spell, and computational cost are compared. Finally, any exhortations are provided on assessed shaft ciphers and implementation platforms.

Key words: Block ciphers, memory and energy utilization efficiency, performance evaluation, wireless sensor networks

© К.Н. Әлібекова[1*], Ж.М. Алимжанова[1], С.С. Байзакова[2], 2023
[1]Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан;
[2]Ы.Алтынсарин атындағы Арқалық педагогикалық институты,
Арқалық, Қазақстан.
E-mail: kamalibekova@gmai.com

СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕР ҮШІН БЛОКТЫҚ ШИФРЛАРДЫҢ ӨНІМДІЛІГІН БАҒАЛАУ

Әлібекова Камила Нұрдәулетқызы — PhD Докторанты, Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
E-mail: E-mail: kamalibekova@gmail.com. ORCID: https://orcid.org/0000-0001-5039-7833;
Алимжанова Жанна Муратбековна — Физика-математика ғылымдарының кандидаты, Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы, Қазақстан
E-mail: zhannamen@mail.ru ORCID: https://orcid.org/0000-0001-6282-5356;
Кошпанова Каламкас Ескаткызы — Магистр дәрежесі, аға оқытушы, Ы. Алтынсарин атындағы Арқалық мемлекеттік педагогикалық институты, Арқалық, Қазақстан
E-mail: saule_alikosh@mail.ru.

Аннотация. Қауіпсіздік көптеген сымсыз сенсорлық желі (WSN) қосымшаларындағы негізгі мәселелердің бірі болып табылады. WSNS-те қауіпсіздік қызметтерін ұсыну үшін бірқатар криптографиялық алгоритмдер жасалды. Дегенмен, энергияны үнемдейтін және жеңіл шифрды таңдау сенсорлық түйін ресурстарының шектеулі болуына байланысты қиын міндет болып табылады. Осылайша, криптографиялық алгоритмдерді жүйелі бағалау қауіпсіздік шаралары мен операциялық шығындар арасындағы романы жақсы түсінуді қамтамасыз ету үшін қажет. Бұл мақалада біз бес блоктық шифрды қарастырдық: Skipjack, түзетілген Block tiny шифрлау алгоритмі (XTEA), RC5, кеңейтілген шифрлау стандарты (AES) және хаотикалық карта мен генетикалық операцияларға негізделген шифрлау алгоритмі (CGEA). Бұл шифрлардың өнімділігі Arduino Pro және Mica2 сенсорларының көмегімен бағаланады. Содан кейін жадты пайдалану, жұмыс уақыты және есептеу шығындары салыстырылады. Соңында, бағаланатын блок шифрлары мен іске асыру платформалары бойынша кейбір ұсыныстар беріледі.

Түйін сөздер: Блоктық шифрлар, жад пен энергияны пайдалану тиімділігі, өнімділікті бағалау, сымсыз сенсорлық желілер

© К.Н. Алибекова[1*], Ж.М. Алимжанова[1], С.С. Байзакова[2], 2023
[1]Казахский национальный университет имени аль-Фараби,
Алматы, Казахстан;
[2]Аркалыкский государственный педагогический институт
им. И. Алтынсарина, Аркалык, Казахстан.
E-mail: kamalibekova@gmai.com

ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ БЛОЧНЫХ ШИФРОВ ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ

Әлібекова Камила Нұрдәулетқызы — Докторант PhD, Казахский национальный университет им. Аль-Фараби, Алматы, Казахстан
E-mail: E-mail: kamalibekova@gmail.com. ORCID: https://orcid.org/0000-0001-5039-7833;
Алимжанова Жанна Муратбековна — Кандидат физико-математических наук, Казахский национальный университет им. Аль-Фараби, Алматы, Казахстан
E-mail: zhannamen@mail.ru. ORCID: https://orcid.org/0000-0001-6282-5356;
Кошпанова Каламкас Ескаткызы — Степень магистра, старший преподаватель, Аркалыкский государственный педагогический институт им. И. Алтынсарина, Аркалык, Казахстан
E-mail: saule_alikosh@mail.ru.

Аннотация. Безопасность является одной из основных проблем во многих приложениях беспроводной сенсорной сети (WSN). Для предоставления услуг безопасности в WSNS был разработан ряд криптографических алгоритмов. Однако выбор энергоэффективного и легкого шифра является сложной задачей из-за ограниченности ресурсов сенсорных узлов. Таким образом, систематическая оценка криптографических алгоритмов необходима для обеспечения хорошего понимания компромисса между показателями безопасности и эксплуатационными расходами. В этой статье мы рассмотрели пять блочных шифров: Skipjack, исправленный алгоритм шифрования Block Tiny (XTEA), RC5, расширенный стандарт шифрования (AES) и алгоритм шифрования на основе хаотической карты и генетических операций (CGEA). Производительность этих шифров оценивается с помощью датчиков Arduino Pro и Mica2. Затем сравниваются использование памяти, время работы и вычислительные затраты. Наконец, даются некоторые рекомендации по оцениваемым блочным шифрам и платформам реализации.

Ключевые слова: блочные шифры, эффективность использования памяти и энергии, оценка производительности, беспроводные сенсорные сети

Кіріспе

Сымсыз сенсорлық желілер дұшпандық ортада кездейсоқ орналастырылатын көптеген арзан сенсорлық түйіндерден (SNS) тұрады (Mojisola, 2022). Батареямен жұмыс істейтін бұл SNS-тердің жадысы аз, процессорлары әлсіз және байланыс мүмкіндіктері шектеуліболып келеді. Сондықтан соңғы бірнеше жылда WSNs-те энергия тиімділігіне қол жеткізу үшін бірқатар

қауіпсіз және жеңіл блоктық шифрлар ұсынылды. Алайда, эксперименттік нәтижелер бұл шифрлардың көпшілігінің әдеттегі шифрлармен салыстырғанда өнімділігі төмен екенін көрсетеді (Soni, 2019) Осылайша, өнімділікті бағалау әртүрлі криптографиялық схемалардың эталонын қамтамасыз ету үшін маңызды.

Қауіпсіздік саясатын енгізу шығындар мен өнімділіктің сақталуын қамтамасыз етуі керек. Мысалы, көптеген WSN қосымшалары қауіпсіздіктің жоғарылауын қамтамасыз ету үшін күрделі криптографиялық алгоритмдерді қажет етеді. Алайда, криптожүйені іске асыру үшін қуатты SNS қажет болғандықтан, шығындар артады. Сондықтан іске асыру шығындары мен тиімділік арасындағы байланысты нақты түсіну қажет. 1-кестеде кеңінен қолданылатын сенсорлық құрылғылардың бірқатар жабдықтарының құны мен техникалық сипаттамалары туралы салыстырмалы мәліметтер келтірілген. Кестеден EZ430-RF2500 және Arduino Pro motes арзанырақ екенін көруге болады, бірақ олардың жады да аз. Демек, арзан SNS-те криптографиялық схемалардың өнімділігін бағалау экономикалық тиімді платформалар құру мүмкіндігін зерттеу үшін қажет.

Бұл мақалада нақты сенсорлық жабдыққа негізделген криптографиялық алгоритмдерді эксперименттік бағалау ұсынылған. Жад тиімділігін, есептеу шығындарын және жұмыс уақытын салыстыру үшін Mica2 және Arduino Pro mote платформаларында бірқатар блоктық шифрлар енгізілген. Соңында, эксперимент нәтижелеріне сүйене отырып, ең жақсы криптографиялық алгоритм мен іске асыру платформасын таңдау үшін пайдалы болатын кейбір маңызды тұжырымдар беріледі. Құжаттың қалған бөлігі келесідей ұйымдастырылған: 2-бөлімде сәйкесінше сипатталған жұмыс істейді. 3-бөлімде WSNs-те бағаланатын блоктық шифрларға шолу берілген. 4-бөлімде енгізу платформалары егжей-тегжейлі сипатталған. Тиімділікті бағалау және талдау 5-бөлімде ұсынылған. 6-бөлімде құжат талқыланады және аяқталады.

Атауы	Бағасы (USD)	Пакеті (incl.)	Микро-контроллер	Жолы (bits)	Уақыты (MHz)	RAM (KB)	Жылдам-дығы (KB)	EEPROM (KB)
SHIMMER	226	2 boards	MSP430F1611	16	4-8	10	48	None
Waspmote	168	4 sensors	ATmega1281	8	14	8	128	4
TelosB	102	3 sensors	MSP430F1611	16	4-8	10	48	1024
Mica2	99	N/Av.	ATmega128L	8	8	4	128	512
EZ430-RF2500	40	Board only	MSP430F2274	16	16	1	32	None
Arduino Pro (328)	25	nrf24L01 radio	ATmega328	8	8-16	2	32	1

Кесте 1. Жабдықтың құны және техникалық сипаттамалары

Әдебиеттерге шолу

WSNs үшін қауіпсіздік қасиеттерін де, жад пен блоктық Шифр энергиясын пайдалану тиімділігін де ескеретін жүйелі бағалау жүйесін ұсынады. Авторлар rijndael cipher-ді қауіпсіздік пен энергия тиімділігін қамтамасыз ету үшін пайдалануды ұсынады, ал misty1 деректерді сақтау және энергия тиімділігін арттыру үшін ұсынылады

Криптографиялық хэш функцияларының (MD5 және SHA1) өнімділігін, сондай-ақ шифрлау алгоритмін (AES) талдау үшін сынақ стендін пайдалану қажет. Нәтижелер криптографиялық алгоритм 1 КБ массиві бар бір AES операциясы үшін 1,67 с сияқты ұзақ жұмыс уақытын қажет ететінін көрсетеді.

Салыстырмалы өнімділік талдауы (Sun, 2007) rc6, AES және масштабталатын шифрлау алгоритмі (SEA) sea AES және RC6 шифрларымен салыстырғанда аз жадты қажет ететінін көрсетеді, ал AES және RC6 сәйкесінше жұмыс уақыты мен өткізу қабілеттілігін пайдалану тұрғысынан ең жақсы өнімділікке қол жеткізеді.

Симметриялы кілттері бар шифрларға арналған энергияның есептеу шығындары әр түрлі блок өлшемдері мен пайдалы жүктемелерді ескере отырып есептеледі және салыстырылады (Segar, 2013) Сонымен қатар, авторлар қауіпсіздікті де, энергия тиімділігін де қамтамасыз ету үшін байт-бағдарланған ауыстыру-ауыстыру желілік шифрын (SPN) пайдалануды ұсынады. Симметриялық блок шифрларының WSN өнімділігі мен мінез-құлқына әсері желінің маңызды параметрлерін анықтау үшін талданады (Babenko, 1999). AES, RC5 және Skipjack шифрлары MicaZ және TelosB чиптерінде жүзеге асырылады, сонымен қатар сапалық және сандық жағынан маңызды компаға келеді

Mica2 сенсорларының шаңындағы AES, RC5 және RC6 алгоритмдерінің жад тиімділігін, жұмыс уақытын және қуат тұтынуын өлшеп, салыстырды. Эксперименттердің нәтижелері RC5 уақыт пен энергия тиімділігі тұрғысынан ең қолайлы блоктық Шифр екенін көрсетеді. Кәдімгі криптографиялық алгоритмдерден басқа, Mica2 motes-те HIGH (Schneier, 2002) Simple Lightweight Encryption (Scheme Koo, 2008) және Lightweight Security Protocol (Biswas, 2014) сияқты бірнеше жеңіл блоктық шифрлар енгізілген. Бұл алгоритмдер энергияны үнемдейді және WSNS-те қауіпсіздіктің жақсы деңгейін қамтамасыз етеді. Бұл жұмыс екі түрлі аппараттық платформада бірқатар блоктық шифрларды жүзеге асырады және қауіпсіздік көрсеткіштері мен пайдалану шығындарын зерттейді. Эксперименттік нәтижелер бағаланған блоктық шифрлардың тиімділігін көрсетеді.

Блоктық шифрлар	Ұзындық кілті (биттер)	Раундтар	Блоктың ұзындығы (биттер)
Skipjack	80	32	64
XXTEA	128	14	64
RC5	128	14	64
AES-128	128	10	128

AES-256	256	14	128
CGEA	256	N/Av.	128

Кесте 2. Эксперименттерде қолданылатын шифр параметрлері

Материалдар мен әдістер

Бұл бөлімде skipjack, XXTEA, RC5, AES және CGEA шифрлары сипатталған. 2-кестеде біздің тәжірибелеріміздегі әрбір блок шифры үшін қабылданған параметрлер келтірілген.

Skipjack 64 биттік деректер блоктары үшін 80 биттік кілтті пайдаланады. Онда 32 раундтық теңгерімсіз фейстель желісі бар. Бихам және басқалар 32-ден 31-ге қарсы шабуыл жасады мүмкін емес дифференциалды криптоанализді қолданатын раундтар (Biswas, 2014). Сонымен қатар, кілттің қысқа ұзындығы Skipjack-ті толық кілт іздеумен шабуылдарға осал етеді.

XXTEA 64 биттік блок ұзындығына және 128 биттік кілт ұзындығына ие. Онда раундтардың ауыспалы саны бар (6-дан 32-ге дейін толық цикл) теңгерімсіз Фейстель желісі жүзеге асырылады. Толық функционалды xxtea-ға соңғы тіркелген шабуыл-бұл 259 сұранысты қолдана отырып, дифференциалды криптоанализге негізделген таңдалған ашық мәтіндік Шабуыл (Biham, 2005).

RC5-айнымалы параметрлері бар икемді блок шифры: блок өлшемі (32, 64 немесе 128 бит), кілт өлшемі (0-ден 2040 битке дейін) және раундтар саны (0-ден 255-ке дейін). Бұл WSNs-те кеңінен қолданылатын блоктық шифр. Алайда, 64 биттік блоктары бар 12 раундтық RC5 таңдалған 244 ашық мәтінді қолдана отырып, дифференциалды шабуылға осал (Yarrkov, 1998).

AES-бұл ауыстыру-ауыстыру желісіне негізделген және 128 биттік блоктың бекітілген өлшемі бар қайталанатын блок шифры. Ол 4 × 4 байт массивімен жұмыс істейді. Сәйкесінше 128, 192 және 256 биттік кілттер үшін 10, 12 және 14 раундтарда жұмыс істейтін AES осал (Polley, 2004).

CGIAR-жалған кездейсоқ биттер тізбегін жасау үшін хаотикалық картаны пайдаланатын жеңіл блоктық шифр (Wu) 256 биттік реттілік блоктары 128 биттік деректер блоктарын шифрлау немесе шифрын ашу үшін кілт ретінде пайдаланылады. Алгоритм шифрланған мәтінді құру үшін XOR, мутация және ашық мәтінді қиылысу операцияларын жүзеге асырады. Раундтарды пайдаланудың орнына ол әрбір деректер байты үшін қиылысу әрекетін ашық мәтін ретінде орындайды.

Жабдықтың сипаттамасы

Arduino Pro-atmega168/328 негізіндегі микроконтроллер тақтасы (Biswas, 2013) Тәжірибелер келесі конфигурацияларда USB қуатымен жұмыс істейтін Arduino Pro (328) чиптерін қолданды: жұмыс кернеуі - 3,3 В, сағат жиілігі - МГц, жедел жады - 2 Кб, ФЛЭШ-жады - 32 Кб, EEPROM - 1 Кб, радио құрылғысы - nrf24L01 және деректер жылдамдығы - 19,2 Кбит/с Mica2 - бұл atmega128l процессорына негізделген төмен қуатты Mote сенсоры (Cazorla,

2013). Тәжірибелер келесі конфигурацияларда USB қуаты бар Mica2 чиптерін пайдаланды: жұмыс кернеуі - 3,3 В, сағат жиілігі - 8 МГц, жедел жады - 4 КБ, флэш-жады - 128 Кб, EEPROM - 512 Кб, радио құрылғысы - CC1000 және деректер жылдамдығы - 19,2 Кбит/с.

Бағдарламалық жасақтаманың сипаттамасы

Әр блоктық шифрдың бастапқы коды Arduino IDE-де Arduino Promotions-қа құрастыру және жүктеу үшін жазылады. Біздің тәжірибелерімізде екі кіріктірілген кітапхана функциясы (microsecondsToClockCycles() және Serial қолданылды. print()) процессор циклдары мен шифрлау уақытын алу және басып шығару үшін қолданылады. Mica2 чиптерінде шифрларды енгізу үшін компоненттерге негізделген жоғары деңгейлі бағдарламалау тілі (nesC) қолданылады (Young Adam and Moti Yung, 2005)..Жергілікті Уақыт Функциялары.get() және printf () жұмыс уақытын алу үшін пайдаланылады, ал процессор циклдары ATEMU [20] арқылы алынады.

Сурет. 1. Эксперименттік орнату: (а) USB қуаты бар Mica2 mote, (б) Arduino Pro бағдарламалаушы тақтасы бар USB қуаты бар mote, (с) батареямен жұмыс істейтін Arduino Promote

Соңында, AVR-size және AVR-objdump утилиталары сәйкесінше Arduino Pro және Mica2 motes құрылғыларында жадты пайдалануды өлшеу үшін қолданылады. Бұл екі утилита көрсетеді

нысан файлдарының тақырыптары туралы ақпарат. Ақпарат мәтінге, деректерге және bss бөліміне қатысты жедел жад пен ROM өлшемін қамтиды.

Тиімділікті бағалау және талдау

Блоктық шифрлар	Mica2	Arduino Pro
Skipjack	9820	12672
XXTEA	24064	30464

RC5	53014	61504
AES-128	37525	43200
AES-256	80344	88896
CGEA	67786	76212

Бұл бөлімде Mica2 және Arduino Promotions бағдарламаларында іске асырылған оңтайландырылған skipjack, XXTEA, RC5, AES және CGEA блок шифрларының салыстырмалы өнімділігі талдауы берілген. Салыстыру үшін үш маңызды параметр таңдалды: жадты тұтыну, есептеу шығындары және жұмыс уақыты.

Блоктық шифрлар	Mica2		Arduino Pro	
	RAM	ROM	RAM	ROM
Skipjack	3096	8658	398	4952
XXTEA	542	6312	226	4112
RC5	682	6110	350	3184
AES-128	1074	6296	814	3692
AES-256	1822	7932	1014	4190
CGEA	664	6268	548	3228

Жадты тұтыну

Жадты тұтыну-бұл аз жадты шифрлау алгоритмдерін таңдау үшін қолдануға болатын маңызды өнімділік көрсеткіші. 3-кестеде Mica2 және Arduino Pro платформаларында әрбір блок шифры тұтынатын жад көлемі көрсетілген. Skipjack және AES-256 басқа алгоритмдермен салыстырғанда көбірек жадты қажет ететінін көруге болады. AES-128 жадына қойылатын талаптар AES-256-мен салыстырғанда сәл төмен, ал RC5 барлық алгоритмдердің ішіндегі ең жеңілі.

Сындар - Skipjack және AES екеуі де 256 байтты үлкен s-блокты пайдаланады, нәтижесінде Алгоритмдер айтарлықтай жадты алады. Xxtea, RC5 және CGEA орындау үшін аз жадты қажет етеді, сондықтан Arduino Pro сияқты шектеулі жады бар SNS үшін қолайлы. Бір маңызды байқау-Arduino Promote-те AES-256 енгізу қол жетімді жадтың жетіспеушілігі туралы хабарламаны көрсетеді. Демек, артық жадты қолданатын криптографиялық Алгоритмдер Arduino Pro платформасында тұрақтылық мәселелеріне тап болуы мүмкін.

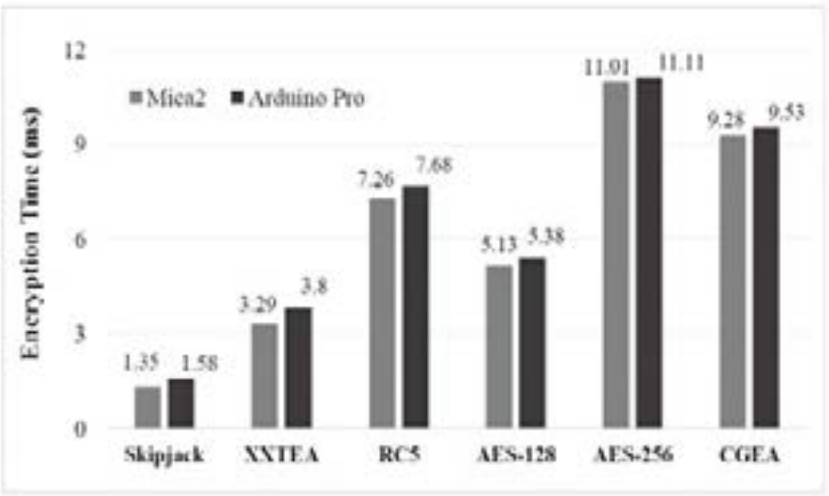
Есептеу шығындары

Алгоритмнің энергетикалық тиімділігін оның есептеу күрделілігіне қарай есептеуге болады. Процессор циклі үшін энергияны тұтыну тұрақты деп есептесек, оның мөлшері бір Байт үшін тұтынылатын энергияны бір Байт ашық мәтінді өңдеуге қажетті процессор циклдарының санын өлшеу арқылы есептеуге болады. Алайда, 4-кестеде жалпы саны көрсетілген 32 байт деректерді шифрлау үшін әр алгоритм талап ететін процессор циклдарының саны. Skipjack-бұл энергияны үнемдейтін блок-Шифр, ал AES-256 өнімділігі

барлық алгоритмдердің ішіндегі ең нашар екенін көруге болады. Сондай-ақ, AES 128 AES-256-дан екі есе жақсы жұмыс істейтіні атап өтілді.

Сын-кілттің өлшемі мен раундтар саны есептеу күрделілігінде маңызды рөл атқарады. AES-128 блок шифрын енгізу кілттің кішігірім өлшемі мен раундтардың аздығына байланысты AES-256 талап ететін есептеу шығындарының жартысынан көбін азайтады. Сондай-ақ, RC5 бірдей өлшемді кілттің болуына қарамастан, AES-128-мен салыстырғанда процессордың көп циклін тұтынады. Себебі, RC5 14 раундты орындайды, ал AES-128 тек 10 раундты пайдаланады.

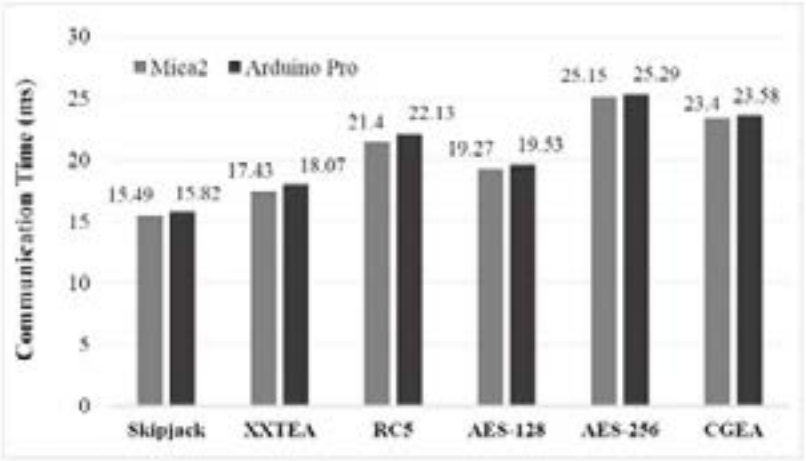
Сурет. 2. Шифрлау уақыты



Пайдалану шығындары

Жұмыс жылдамдығы уақытты пайдалану тиімділігін көрсетеді және шифрлау уақыты мен байланыс уақыты бойынша анықталады. Шифрлау уақыты-ашық мәтінді шифрлауға кететін уақыт мөлшері, ал шифрланған мәтінді шифрлауға және сәтті жіберуге кететін уақыт Байланыс уақыты ретінде анықталады. Інжір. 2 32 байтты деректерді шифрлау үшін қажетті жұмыс уақыты көрсетілген. Skipjack сәйкесінше AES және CGEA шифрларымен салыстырғанда 7 және 6 есе жылдам жұмыс істейтінін көруге болады. Сонымен қатар, AES-128 шифры AES-256-мен салыстырғанда шифрлау уақытын жартысынан астамға қысқартады. Дәл осындай нәтижелер суретте көрсетілгендей байланыс уақыты эксперименті үшін алынған.

Сурет. 3. Байланыс уақыты



Қорытынды

Эксперимент нәтижелеріне сәйкес, RC5 жад тұрғысынан ең тиімді блоктық Шифр болып табылады. Xxtea және CGEA сонымен қатар Arduino Pro сияқты жады шектеулі SNS үшін әлеуетті үміткерлер болып табылады. Екінші жағынан, Skipjack жұмыс уақыты мен есептеу шығындары бойынша ең жақсы өнімділікті көрсетеді. Xxtea және AES-128 шифрлары да аз қуат тұтынады. Алайда, қауіпсіздік тұрғысынан Skipjack-бұл кілттің қысқа ұзындығына байланысты жоғары тәуекел алгоритмі. Сол сияқты, XXTEA және RC5 уақыт шабуылы және таңдалған ашық мәтінді қолданатын шабуыл сияқты бірқатар қауіпсіздік шабуылдарына осал. Сонымен қатар, 128 биттік кілт кванттық шабуылдан қорғалмайды. Кванттық есептеу жүйелері 264 секундта 128 биттік кілтті бұзуға қабілетті (Somsuk Kritsanapong, 2021). Дегенмен, AES256 және CGEA 256 биттік кілттің арқасында әлі де толық іздеуден қорғалған болады ұзындығы. Сондықтан қауіпсіздік басымдыққа ие болған кезде AES-256 немесе CGEA блок шифрларын пайдалануды ұсынамыз. RC5, XXTEA және AES-128 шифрларын қауіпсіздіктің минималды деңгейін қажет ететін қосымшалар үшін пайдалануға болады.

Бұлмақаладаskipjack,XXTEA,RC5,AESжәнеCGEAблоктықшифрларының салыстырмалы өнімділігі талдауы берілген. Айта кету керек, Arduino Pro mica2-ге қарағанда сәл ұзағырақ жұмыс уақыты мен байланысты қажет етеді, бұл шамалы. Осылайша, көп уақыт пен жадты қажет ететін қолданбалардың орнына қоршаған ортаны бақылау сияқты жалпы WSN қолданбалары үшін Arduino Pro пайдалану үнемді болады. Болашақ жұмысымызда біз ағындық шифрлардың өнімділігін бағалаймыз және нәтижелерді блоктық шифрлармен салыстырамыз.

REFERENCES

Babenko J1.K., 1999. Methodical manual: Introduction to the specialty "Organization and technology of information protection" Taganrog: TRTU, 1999. № 2800 E. Biham, A. Shamir: "Differential Cryptanalysis of the Full 16-round DES", Crypto'92, Springer-Velgar, 1998, p. 487.

Biswas K., Muthukkumarasamy V., Sithirasenan E., Singh K., 2014. A simple lightweight encryption scheme for WSNs. In: Chatterjee, M., Cao, J., Kothapalli, K., Rajsbaum, S. (eds.) ICDCN. LNCS. Vol. 8314. Pp. 499–504. Springer, Heidelberg (2014).

Biswas K., 2014. Lightweight security protocol for WSNs. In: International Symposium on WoWMoM. Pp. 1–2, Sydney (2014).

Biham E., Biryukov A., Shamir A., 2005. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In: J. of crypt. 18(4). Pp. 291–311 (2005).

Biswas K., Muthukkumarasamy V., Sithirasenan E., 2013. Maximal clique based clustering scheme for WSNs. In: IEEE ISSNIP. Pp. 237–241, Melbourne (2013).

Cazorla M., Marquet K., Minier M., 2013. Survey and benchmark of lightweight block ciphers for WSNs. In: SECRYPT, (2013)

Intila C., Gerardo B., Medina R., 2019. A study of public key 'e' in RSA algorithm //IOP Conference Series: Materials Science and Engineering. – IOP Publishing, 2019. – T. 482. – №. 1. – P. 012016.

Koo W.K., Lee H., Kim Y.H., Lee D.H., 2008. Implementation and analysis of new lightweight cryptographic algorithm suitable for WSNs. In: ISA. Pp. 73–76, (2008).

Lee G. et al., 2019. PyWavelets: A Python package for wavelet analysis //Journal of Open Source Software. – 2019. – T. 4. – №. 36. – P. 1237.

Mojisola F.O. et al., 2022. An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA) //Egyptian Informatics Journal. – 2022.

Polley J., Blazakis D., Mcgee J., Rusk D., Baras J.S., 2004. ATEMU: a fine grained sensor network simulator. In: IEEE SECON. Pp. 145–152, (2004).

Soni G.K., Arora H., Jain B., 2019. A novel image encryption technique using Arnold transform and asymmetric RSA algorithm //International Conference on Artificial Intelligence: Advances and Applications 2019. – Springer, Singapore, 2020. – Pp. 83–90.

Somsuk Kritsanapong, 2021. "A New Methodology to Find Private Key of RSA Based on Euler Totient Function." Baghdad Science Journal 18.2 (2021). Pp. 338–348.

Segar T.C., Vijayaragavan R., 2013. Pell's RSA key generation and its security analysis //2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT). – IEEE, 2013. – Pp. 1–5.

Schneier B., 2002. Applied Cryptography. Protocols, algorithms, source texts in C. M.: TRIUMPH Publishing House, 2002.

Sun H.M. et al., 2007. Dual RSA and its security analysis //IEEE Transactions on Information Theory. – 2007. – T. 53. – №. 8. – Pp. 2922–2933.

Thangavel M. et al., 2015. An enhanced and secured RSA key generation scheme (ESRKGS) // Journal of information security and applications. – 2015. – T. 20. – Pp. 3–10.

Yarrkov E., 1998. Cryptanalysis of XXTEA, http://eprint.iacr.org/2010/254.pdf. Biryukov, A., Kushilevitz, E.: Improved cryptanalysis of RC5. In: N., Kaisa (eds.) EUROCRYPT'98. LNCS. Vol. 1403. Pp. 85–99. Springer, Heidelberg (1998).

Young Adam and Moti Yung, 2005. "A space efficient backdoor in RSA and its applications." International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2005.

Wu D. Introduction to cryptography. In: Lecture Notes, Stanford University, http://crypto.stanford.edu/~dwu4/notes/CS255LectureNotes.pdf

МАЗМҰНЫ

А. Адамова, Т. Жукабаева, Е. Марденов
ЗАТТАР ИНТЕРНЕТІ: ЖЕҢІЛДІК АЛГОРИТМДЕРДІҢ ДАМУЫ ЖӘНЕ БОЛАШАҒЫ.....5

Г. Алпысбай, А. Бедельбаев, О. Усатова, А. Жұмабекова, Эдзард Хофиг
ЗИЯНДЫ БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАРДЫ ТАЛДАУДА МАШИНАЛЫҚ ОҚЫТУ АЛГОРИТМІН ҚОЛДАНУ.....21

А.У. Алтаева, А.Ш. Каипова, А.У. Мухамеджанова, Г.К. Оспанова
МЕДИЦИНАДА ЧАТ-БОТТАРДЫ ҚОЛДАНУ ПЕРСПЕКТИВАЛАРЫ.....32

Г.А. Анарбекова, Н.Н. Оспанова, Д.Ж. Анарбеков
НОРМАЛАНҒАН КІРІС ВЕКТОРЛАРЫ: ДЕРЕКТЕРДІ ДАЙЫНДАУДЫҢ БАСТАПҚЫ КЕЗЕҢІ.....40

А.Е. Әбжанова, А.И. Такуадина, С.К. Сагнаева, С.К. Серикбаева, Г.Т. Азиева
ТОПЫРАҚТЫ ТЕХНИКАЛЫҚ МЕЛИОРАЦИЯЛАУ ӘДІСТЕРІНДЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ПАЙДАЛАНУ.....55

К.Н. Әлібекова, Ж.М. Алимжанова, С.С. Байзакова
СЫМСЫЗ СЕНСОРЛЫҚ ЖЕЛІЛЕР ҮШІН БЛОКТЫҚ ШИФРЛАРДЫҢ ӨНІМДІЛІГІН БАҒАЛАУ.....70

К.Б. Багитова, Ш.Ж. Мүсіралиева, М.А. Болатбек, Р.Қ. Оспанов
ИНТЕРНЕТТЕ ЭКСТРЕМИСТІК МАЗМҰНДЫ АНЫҚТАУҒА АРНАЛҒАН EXWEB БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАМАСЫН ӘЗІРЛЕУ.....81

А.Ш. Баракова, О.А. Усатова, А.С. Орынбаева
ВЕБ САЙТТАРДАҒЫ САНДЫҚ РЕСУРСТАРДЫ СТЕГАНОГРАФИЯ ӘДІСІМЕН ҚОРҒАУДЫҢ МОДЕЛІ.....96

А.С. Омарбекова, А.Е. Назырова, Н. Тасболатұлы, Б.Ш. Разахова
ИНТЕЛЛЕКТУАЛДЫ ELEARNING ЖҮЙЕСІНІҢ ОНТОЛОГИЯЛЫҚ МОДЕЛІ ЖӘНЕ ОҚЫТУ НӘТИЖЕЛЕРІ.....108

М.Қ. Болсынбек, Г.Б. Абдикеримова, С.К. Серикбаева, А.Ж. Танирбергенов, Ж.К. Тасжурекова
ТОПЫРАҚ ЖӘНЕ ТОПЫРАҚ ЭРОЗИСЫН БОЛЖАУЖЫҢ АҚПАРАТТЫҚ ЖҮЙЕЛЕРІ МЕН ӘДІСТЕРІН ЗЕРТТЕУ.....128

Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Б.А. Ху Вен-Цен
LSTM ЖӘНЕ GRU ҮЛГІЛЕРІ НЕГІЗІНДЕ ҚАЗАҚ ДАКТИЛЬДЕРІН ТАНУДЫҢ ИНТЕЛЛЕКТУАЛДЫ ЖҮЙЕСІН ҚҰРУ.....141

М.Д. Кабибуллин, **Б.Б. Оразбаев**, **К.Н. Оразбаева**, **С.Ш. Искакова**, **Ж.Ш. Аманбаева**
КҮРДЕЛІ ХИМИЯЛЫҚ-ТЕХНОЛОГИЯЛЫҚ ЖҮЙЕЛЕР АГРЕГАТТАРЫНЫҢ МОДЕЛЬДЕРІН БАСТАПҚЫ АҚПАРАТТЫҢ ЖЕТІСПЕУШІЛІГІ МЕН АЙҚЫНСЫЗДЫҒЫ ЖАҒДАЙЫНДА ҚҰРУ.....154

М.Ж. Қалдарова, А.С. Аканова, М.Г. Гриф, У.Ж. Айтимова, А.С. Муканова
ТОПЫРАҚ ЖАҒДАЙЫН БАҒАЛАУ ҮШІН ҚОЛДАНЫЛАТЫН ҒАРЫШТЫҚ СУРЕТТЕРДІ ӨҢДЕУ АЛГОРИТМДЕРІ МЕН ӘДІСТЕРІ.....172

К. Келесбаев, Ш. Раманкулов, М. Нуризинова, А. Паттаев, Н. Мұсахан
STEM ЖОБАЛЫҚ ОҚЫТУДЫҢ БОЛАШАҚ ФИЗИКА МАМАНДАРЫН ДАЯРЛАУДАҒЫ ЕРЕКШЕЛІКТЕРІ.....193

А.Е. Кулакаева, Е.А. Дайнеко, А.З. Айтмагамбетов, А.Т. Жетписбаева, Б.А. Кожахметова
ШАҒЫН ҒАРЫШ АППАРАТЫ ОРБИТАСЫНЫҢ СИПАТТАМАЛАРЫНЫҢ СПУТНИКТІК РАДИО МОНИТОРИНГ ЖҮЙЕСІНІҢ ПАРАМЕТРЛЕРІНЕ ӘСЕРІ ТУРАЛЫ.....208

А.Е. Назырова, Г.Т. Бекманова, А.С. Муканова, Н. Амангелді, М.Ж. Калдарова
БІЛІМ БЕРУ БАҒДАРЛАМАЛАРЫ ҮШІН АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕНІ ӘЗІРЛЕУ.....221

А.Б. Тоқтарова, Б.С. Омаров, Ж.Ж. Ажибекова, Г.И. Бейсенова, Р.Б. Абдрахманов
ОНЛАЙН КОНТЕНТТЕГІ БЕЙӘДЕП СӨЗДЕР МӘЛІМЕТТЕР ҚОРЫН DATA MINING АРҚЫЛЫ АНАЛИЗДЕУ.....237

Ә.Б. Тынымбаев, К.С. Байшоланова, К.Е. Кубаев
АҚПАРАТТЫ ҚОРҒАУ ЖҮЙЕЛЕРІНДЕГІ NAVIVE BAYESIAN ЖІКТІТУШІСІН ҚОЛДАНУ.....252

Г.Қ. Шаметова, А.Ә. Шәріпбай, Б.Ғ. Сайлау
ҚОЛЖЕТІМДІЛІКТІ БАСҚАРУ ЖҮЙЕЛЕРІНДЕГІ ҚҰПИЯНЫ БӨЛУДІҢ КРИПТОГРАФИЯЛЫҚ СҰЛБАЛАРЫН ТАЛДАУ.....261

Г.Б. Абдикеримова, А.Ә. Шекербек, М.Г. Байбулова, С.К. Абдикаримова, Ш.Ш. Жолдасова
КЕУДЕ ПАТОЛОГИЯСЫН АВТОКОРРЕЛЯЦИЯЛЫҚ ФУНКЦИЯ АРҚЫЛЫ АНЫҚТАУ.....274

СОДЕРЖАНИЕ

А. Адамова, Т. Жукабаева, Е. Марденов
ИНТЕРНЕТ ВЕЩЕЙ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЛЕГКОВЕСНЫХ АЛГОРИТМОВ.....5

Г. Алпысбай, А. Бедельбаев, О. Усатова, А. Жумабекова, Эдзард Хофиг
ПРИМЕНЕНИЕ АЛГОРИТМА МАШИННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА ВРЕДОНОСНОГО ПО.....21

А.У. Алтаева, А.Ш. Каипова, А.У. Мухамеджанова, Г.К. Оспанова
ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЧАТ-БОТОВ В МЕДИЦИНЕ.....32

Г.А. Анарбекова, Н.Н. Оспанова*, Д.Ж. Анарбеков
НОРМАЛИЗОВАННЫЕ ВХОДНЫЕ ВЕКТОРЫ: ПЕРВИЧНЫЙ ЭТАП ПОДГОТОВКИ ДАННЫХ.....40

А.Е. Абжанова, А.И. Такуадина, С.К. Сагнаева, С.К. Серикбаева, Г.Т. Азиева
ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ В МЕТОДАХ ТЕХНИЧЕСКИХ МЕЛИОРАЦИЙ ГРУНТОВ.....55

К.Н. Алибекова, Ж.М. Алимжанова, С.С. Байзакова
ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ БЛОЧНЫХ ШИФРОВ ДЛЯ БЕСПРОВОДНЫХ СЕНСОРНЫХ СЕТЕЙ.....70

К.Б. Багитова, Ш.Ж. Мусиралиева, М.А. Болатбек, Р.К. Оспанов
РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ EXWEB ДЛЯ ВЫЯВЛЕНИЯ ЭКСТРЕМИСТСКОГО КОНТЕНТА В СЕТИ ИНТЕРНЕТ.....81

А.Ш. Баракова, О.А. Усатова, А.С. Орынбаева
РАЗРАБОТКА МОДЕЛИ ЗАЩИТЫ ЦИФРОВЫХ WEB РЕСУРСОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СТЕГАНОГРАФИИ.....96

А.С. Омарбекова, А.Е. Назырова, Н. Тасболатұлы, Б.Ш. Разахова
ОНТОЛОГИЧЕСКАЯ МОДЕЛЬ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ И РЕЗУЛЬТАТЫ ОБУЧЕНИЯ.....108

М.Қ. Болсынбек, Г.Б. Абдикеримова, С.К. Серикбаева, А.Ж. Танирбергенов, Ж.К. Тасжурекова
ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И МЕТОДОВ ПРОГНОЗИРОВАНИЯ ПОЧВЕННОЙ И ПОЧВЕННОЙ ЭРОЗИИ.....128

Л.З. Жолшиева, Т.К. Жукабаева, Ш. Тураев, М.А. Бердиева, Б.А. Ху Вен-Цен
РАЗРАБОТКА ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ КАЗАХСКИХ ДАКТИЛЬНЫХ ЖЕСТОВ НА ОСНОВЕ МОДЕЛЕЙ LSTM И GRU.....141

М.Д. Кабибуллин, Б.Б. Оразбаев, К.Н. Оразбаева, С.Ш. Искакова, Ж.Ш. Аманбаева
РАЗРАБОТКА МОДЕЛЕЙ АГРЕГАТОВ СЛОЖНЫХ ХИМИКО-ТЕХНОЛОГИЧЕСКИХ СИСТЕМ В УСЛОВИЯХ ДЕФИЦИТА И НЕЧЕТКОСТИ ИСХОДНОЙ ИНФОРМАЦИИ.....154

М.Ж. Калдарова, А.С. Аканова, М.Г. Гриф, У.Ж. Айтимова, А.С. Муканова
АЛГОРИТМЫ И МЕТОДЫ ОБРАБОТКИ КОСМИЧЕСКИХ СНИМКОВ ДЛЯ ОЦЕНКИ СОСТОЯНИЯ ПОЧВ.....172

К. Келесбаев, Ш. Раманкулов, М. Нуризинова, А. Паттаев, Н. Мұсахан
ОСОБЕННОСТИ ПРОЕКТНОГО ОБУЧЕНИЯ STEM В ПОДГОТОВКЕ БУДУЩИХ СПЕЦИАЛИСТОВ ПО ФИЗИКЕ.....193

А.Е. Кулакаева, Е.А. Дайнеко, А.З. Айтмагамбетов, А.Т. Жетписбаева, Б.А. Кожахметова
О ВЛИЯНИИ ХАРАКТЕРИСТИК ОРБИТЫ МАЛОГО КОСМИЧЕСКОГО АППАРАТА НА ПАРАМЕТРЫ СИСТЕМЫ СПУТНИКОВОГО РАДИОМОНИТОРИНГА.....208

А.Е. Назырова, Г.Т. Бекманова, А.С. Муканова, Н. Амангелді , М.Ж. Калдарова,
РАЗРАБОТКА АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ДЛЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ.....221

А.Б. Токтарова, Б.С. Омаров, Ж.Ж. Ажибекова, Г.И. Бейсенова, Р.Б. Абдрахманов
АНАЛИЗ НЕОБРАЗНЫХ СЛОВ В ОНЛАЙН-КОНТЕНТЕ С ПОМОЩЬЮ DATA MINING.....237

Ә.Б. Тынымбаев, К.С. Байшоланова, К.Е. Кубаев
ПРИМЕНЕНИЕ НАИВНОГО БАЙЕСОВСКОГО КЛАССИФИКАТОРА В СИСТЕМАХ ЗАЩИТЫ ИНФОРМАЦИИ.....252

Г.Қ. Шаметова, А.Ә. Шәріпбай, Б.Ғ. Сайлау
АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СХЕМ РАСПРЕДЕЛЕНИЯ СЕКРЕТОВ В СИСТЕМАХ УПРАВЛЕНИЯ ДОСТУПОМ.....261

Г.Б. Абдикеримова, А.А. Шекербек, М.Г. Байбулова , С.К. Абдикаримова, Ш.Ш. Жолдасова
ОПРЕДЕЛЕНИЕ ГРУДНОЙ ПАТОЛОГИИ С ПОМОЩЬЮ ФУНКЦИИ АВТОКОРРЕЛЯЦИИ.....274

CONTENTS

A. Adamova, T. Zhukabayeva, Y. Mardenov
INTERNET OF THINGS: STATUS AND PROSPECTS FOR THE DEVELOPMENT OF LIGHTWEIGHT ALGORITHMS.....5

G. Alpysbay, A. Bedelbayev, O. Ussatova, A. Zhumabekova, Edzard Höfig
APPLICATION OF MACHINE LEARNING ALGORITHM IN THE ANALYSIS OF MALICIOUS SOFTWARE.....21

A.U. Altaeva, A.S. Kaipova, A.U. Mukhamejanova, G.K. Ospanova
PROSPECTS OF USING CHATBOTS IN MEDICINE.....32

G.A. Anarbekova, N.N. Ospanova, D.Zh. Anarbekov
NORMALIZED INPUT VECTORS: THE PRIMARY STAGE OF DATA PREPARATION.....40

A.E. Abzhanova, A.I. Takuadina, S.K. Sagnaeva, S.K. Serikbayeva, G.T. Azieva
THE USE OF INFORMATION SYSTEMS IN THE METHODS OF TECHNICAL SOIL RECLAMATION.....55

K. Alibekova, Zh. Alimzhanova, S.S. Baizakova
RATING VALUATION OF BLOCK CIPHERS FOR WIRELESS SENSOR NETWORKS.....70

K.B. Bagitova, Sh.Zh. Mussiraliyeva, M.A. Bolatbek, R.K. Ospanov
DEVELOPMENT OF EXWEB SOFTWARE FOR DETECTING EXTREMIST CONTENT ON THE INTERNET.....81

A.Sh. Barakova, O.A.Usatova, A.S.Orynbaeva
DIGITAL RESOURCES ON WEBSITES MODEL OF PROTECTION BY STEGANOGRAPHY.....96

A.S. Omarbekova, A.E. Nazyrova, N. Tasbolatuly, B.Sh. Razakhova
ONTOLOGICAL MODEL OF AN INTELLIGENT E-LEARNING SYSTEM AND LEARNING OUTCOMES.....108

M. Bolsynbek, G. Abdikerimova, S. Serikbayeva, A. Tanirbergenov, Zh. Taszhurekova
RESEARCH OF INFORMATION SYSTEMS AND METHODS OF FORECASTING SOIL AND SOIL EROSION.....128

L. Zholshiyeva, T. Zhukabayeva, Sh. Turaev, M. Berdieva, B. Khu Ven-Tsen
DEVELOPMENT OF AN INTELLECTUAL SYSTEM FOR RECOGNIZING KAZAKH DACTYL GESTURES BASED ON LSTM AND GRU MODELS.....141

M. Kabibullin, B. Orazbayev, K. Orazbayeva, S. Iskakova, Zh. Amanbayeva
DEVELOPMENT OF MODELS OF UNITS OF COMPLEX CHEMICAL-TECHNOLOGICAL SYSTEMS UNDER CONDITIONS OF DEFICIENCY AND FUZZY OF INITIAL INFORMATION.....154

M.Zh. Kaldarova, A.S. Akanova, M.G. Grif, U.Zh. Aitimova, A.S. Mukanova
ALGORITHM AND METHOD OF PROCESSING SPACE PHOTOS FOR ASSESSMENT OF SOIL.....172

K. Kelesbaev, Sh. Ramankulov, M. Nurizinova, A. Pattaev, N. Mussakhan
FEATURES OF STEAM PROJECT TRAINING IN THE PREPARATION
OF FUTURE SPECIALISTS IN PHYSICS.....193

A.E. Kulakayeva, Y.A. Daineko, A.Z. Aitmagambetov, A.T. Zhetpisbaeva, B.A. Kozhakhmetova
ABOUT THE INFLUENCE OF THE ORBIT CHARACTERISTICS OF A SMALL SPACECRAFT
ON THE PARAMETERS OF THE SATELLITE RADIO MONITORING SYSTEM.....208

A.E. Nazyrova, G.T. Bekmanova, A.S. Mukanova, N. Amangeldi, M.Zh. Kaldarova
DEVELOPMENT OF AN AUTOMATED SYSTEM FOR EDUCATIONAL PROGRAMS.....221

A.B. Toktarova, B.S. Omarov, Zh.Zh. Azhibekova, G.I. Beissenova, R.B. Abdrakhmanov
ANALYSIS OF HATE SPEECH WORDS IN ONLINE CONTENT BY USING
DATA MINING.....237

A.B. Tynymbayev, K.S. Baisholanova, K.Ye. Kubaev
APPLICATION OF NAVIVE BAYESIAN CLASSIFIER IN INFORMATION
PROTECTION SYSTEMS.....252

G.K. Shametova, A.A. Sharipbay, B.G. Sailau
ANALYSIS OF CRYPTOGRAPHIC SECRET DISTRIBUTION SCHEMES IN ACCESS
CONTROL SYSTEMS.....261

G.B. Abdikerimova, A.A. Shekerbek, M.G. Baibulova, S.K. Abdikarimova, Sh.Sh. Zholdassova
CHEST PATHOLOGY DETERMINATION THROUGH AUTOCORRELATION
FUNCTION.....274

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 12.06.2023.
Формат 60х881/8. Бумага офсетная. Печать –ризограф.
19,0 п.л. Тираж 300. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19