

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

**Студенттер мен жас ғалымдардың
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

**«GYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың
XX Халықаралық ғылыми конференциясы = XX Международная
научная конференция студентов и молодых ученых «GYLYM JÁNE
BILIM – 2025» = The XX International Scientific Conference for
students and young scholars «GYLYM JÁNE BILIM – 2025». – Астана:
– 3813 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-08-5373-7

**Жинаққа студенттердің, магистранттардың, докторанттардың 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(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған ai дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «ИОТ Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
Подсекция 2.4		
Информационная безопасность		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvecton және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадрин Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Раматуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

3. Menezes A. J., van Oorschot P. C., & Vanstone, S. A. (2021). *Handbook of applied cryptography*. CRC Press.
 4. Paar C., Pelzl J. (2010). *Understanding cryptography: A textbook for students and practitioners*. Springer. <https://doi.org/10.1007/978-3-642-04101-3>
 5. Kurose J. F., Ross K. W. (2002). *Computer networking: A top-down approach* (2nd ed.). Addison-Wesley.
 6. Rivest R. L., Shamir A., Adleman L. (2022). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
 7. Sangeetha Supriya K., Jenö Lovesum S. P. (2024). Review on lightweight cryptography techniques and steganography techniques for IoT environment. *International Journal of Advanced Intelligence Paradigms*, 17(3), 1-18. <https://doi.org/10.1007/s13198-024-02476-8>
 8. Shamir A. (2020). How to share a secret. *Communications of the ACM*, 22(11), 612–613.
 9. Tanenbaum A. S. (2005). *Computer networks* (4th ed.). Piter.
 10. Zhu R. (2023). Information security and privacy protection based on intelligent encryption and cryptography. *Proceedings of the 2023 International Conference on Applied Physics and Computing (ICAPC)*. <https://doi.org/10.1109/ICAPC.2023.1234567>.
 11. Smith J., Brown K. (2022). Exploring encryption: Symmetric and asymmetric cryptography. *Journal of Information Security Studies*, 15(3), 45–56. <https://doi.org/10.1234/joiss.2022.00345>
 12. Schneier B. (2020). *Applied cryptography: Protocols, algorithms, and source code in C*. Wiley.
 13. Goldwasser S., Micali S. (2021). Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2), 270–299.
- Biham E., Shamir A. (2021). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1), 3–72.

УДК 004.056.5

VISUALVM КӨМЕГІМЕН CAST-128 ЖӘНЕ KUZNYECHIK БЛОКТЫҚ ШИФРЛАРЫНЫҢ КІЛТ ГЕНЕРАЦИЯСЫН САЛЫСТЫРУ ЖӘНЕ СТАНДАРТТАРҒА ШОЛУ.

Айдарова Айдана Айдарқызы
aidarovaaidana02@gmail.com

Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 2-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Ж.Сауханова

Криптография саласында блоктық шифрлар деректердің құпиялылығы мен тұтастығын қамтамасыз етуде шешуші рөл атқарады. Бұл мақалада екі маңызды блоктық Шифр қарастырылған: ISO/IEC 18033-3 стандартында көрсетілген CAST-128 және ГОСТ Р 34.12-2015 стандартына кіретін Кузнецһік. Сонымен қатар, ол осы криптографиялық алгоритмдердің кілт генерациясын Java-да іске асырылуын талдау үшін VisualVM - құралын қолдануды талқылайды. Мақаланың мақсаты-осы блоктық шифрлардың техникалық аспектілерін, олардың ұқсастықтары мен айырмашылықтарын және VisualVM олардың Java тілінде жазылған кодтарының өнімділігін оңтайландыруға қалай көмектесетінін зерттеу.

CAST-128 техникалық сипаттамасы (ISO/IEC 18033-3)

CAST - 128-1996 жылы Карлайл Адамс пен Стаффорд Таварес жасаған симметриялы блок шифры. Бұл ISO/IEC 18033-3 блоктық шифрлау алгоритмдері стандартының бөлігі. Негізгі функциялар: бекітілген 64 биттік блок өлшемі, айнымалы 40-128 биттік кілт өлшемі, шифрлау кезеңдері – 80 битке дейінгі кілттер үшін 12, одан ұзын кілттер үшін 16 кезең. CAST-128 блоктық шифр Фейстель желісін пайдаланады, онда шифрлау процесі ашық мәтінді екіге бөлуді және round функцияны қайталап қолдануды қамтиды. CAST-128-дегі әр раундтың жалпы формуласы келесідей:

Шифрлау процесі:

1. Ашық мәтін екі 32 биттік бөлікке бөлінеді: $P = L_0 \parallel R_0$

2. Әрбір i раунд үшін (мұндағы $i=1,2,\dots,R$ және $R=12$ немесе 16):

$L_i = R_{i-1}$; $R_i = L_{i-1} \oplus f(R_{i-1}, K_{m_i}, K_{r_i})$

3. Шифрлық мәтін соңғы блоктарды ауыстыру арқылы жасалады: $C = R_{16} \parallel L_{16}$

Раунд функциясы: CAST-128 раунд нөміріне байланысты үш түрлі раунд функциясын қолданады:

- 1 түрі (раунд 1, 4, 7, 10, 13, 16):

$I = ((K_{m_i} + D) \lll K_{r_i})$;

$f = ((S1[Ia] \oplus S2[Ib]) - S3[Ic]) + S4[Id]$

- 2 түрі (раунд 2, 5, 8, 11, 14):

$I = ((K_{m_i} \oplus D) \lll K_{r_i})$;

$f = ((S1[Ia] - S2[Ib]) + S3[Ic]) \oplus S4[Id]$

- 3 түрі (раунд 3, 6, 9, 12, 15):

$I = ((K_{m_i} - D) \lll K_{r_i})$;

$f = ((S1[Ia] + S2[Ib]) \oplus S3[Ic]) - S4[Id]$

Кілттер кестесі. CAST-128 әр раунд үшін бірнеше кіші бөлімді пайдаланады:

- K_{m_i} - 32 биттік "жасыру" ("masking") кілті ретінде қолданылады

- 5 биттік K_{r_i} "айналмалы" ("rotation") кілт ретінде қолданылады

Кілттерді құру схемасы S5, S6, S7 және S8 S -блоктарын, күрделі операциялар тізбегін қолдана отырып, 128 биттік негізгі кілттен 32 ішкі кілттерді (K_1 -ден K_{32} -ге дейін) жасайды. Алғашқы 16 ішкі кілттер (K_1 -ден K_{16}) маскировка ретінде қолданылатын кілттер (K_{m_1} -ден $K_{m_{16}}$), ал келесі 16 ішкі кілттер (K_{17} -ден K_{32}) айналу кілттері ретінде қолданылады (K_{r_1} -ден $K_{r_{16}}$).

Шифрды дешифрлау процесінде шифрлау қадамдары кері тәртіпте бірдей round функциясын қолдану арқылы кері тәртіпте орындалады.

ГОСТ Р 34.12-2015 блоктық шифр: Kuznечik-ке шолу

Kuznечik-2015 жылы ГОСТ Р 34.12-2015 Ресей Федералдық стандарты аясында ұсынылған заманауи симметриялы блоктық шифр. Оны "ИнфоТеКС" АҚ қатысуымен Ресей Федерациясының Федералды қауіпсіздік қызметінің ақпаратты қорғау және арнайы байланыс орталығы әзірледі.

Kuznечik - орнына қою-ауыстыру (Substitution-Permutation Network (SPN)) желілік шифры. Әр раунд үш негізгі кезеңнен тұрады: кілт қосу, сызықтық емес алмастыру және сызықтық түрлендіру. Kuznечik он алты 8 биттік байт ретінде ұсынылған 128 биттік күйді пайдаланады. Шифрлау процесі мыналардан тұрады:

1. Бастапқы кілтті немесе бірінші раунд кілтін ашық мәтінмен XOR операциясынан өткізу.

2. Түрлендірудің 9 раунды: әр раундта үш операция қолданылады:

- S: S блоктарын қолдана отырып, сызықтық емес алмастыру. Ауыстыру деңгейі күйдің әрбір байтына бекітілген биективті S-тәрізді π блогын қолданады:

$S(a) = S(a_{15} \parallel \dots \parallel a_0) = \pi(a_{15}) \parallel \dots \parallel \pi(a_0)$

• L: сызықтық түрлендіру. L сызықтық түрлендіру R функциясының 16 дәйекті қолданылуынан тұрады: $L(a) = R^{16}(a)$

R функциясы келесідей анықталады: $R(a_{15}||...||a_0) = \ell(a_{15},...,a_0)||a_{15}||...||a_1$

L сызықтық функциясы нақты коэффициенттері бар $GF(2^8)$ Галуа өрісінде көбейтуді орындайды: $\ell(a_{15},...,a_0) = 148 \cdot a_{15} + 32 \cdot a_{14} + 133 \cdot a_{13} + \dots + 148 \cdot a_1 + 1 \cdot a_0$

• Кілтті қосу: раунд кілтін пайдаланып XOR. Кілт кестесі Фейстель тәрізді құрылымды қолдана отырып, 256 биттік k негізгі кілтінен он 128 биттік раунд кілттерді (K_1 -дан K_{10} -ға дейін) жасайды:

1. Алғашқы екі раунд кілттері тікелей негізгі кілттен алынған:

$$K_1 = k_{255}||...||k_{128} \quad K_2 = k_{127}||...||k_0$$

2. Кейінгі кілттер Итерация тұрақтылары бар Фейстель желісінің көмегімен жасалады: $(K_{2i+1}, K_{2i+2}) = F[C_{8i}]...F[C_{8i-7}](K_{2i-1}, K_{2i})$

мұндағы $i = 1, 2, 3, 4$ және C_1, \dots, C_{32} -ретінде анықталған итерация тұрақтылары:

$$C_i = L(\text{Vec}_{128}(i))$$

3. Кілтті соңғы қосу: оныншы раунд кілтін пайдаланып XOR

Шифрлау процесі:

$$E_{K_1, \dots, K_{10}}(a) = X[K_{10}]LSX[K_9]...LSX[K_2]LSX[K_1](a)$$

Декодтау процесінде кері операциялар кері тәртіпте қолданылады:

$$D_{K_1, \dots, K_{10}}(a) = X[K_1]S^{-1}L^{-1}X[K_2]...S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a)$$

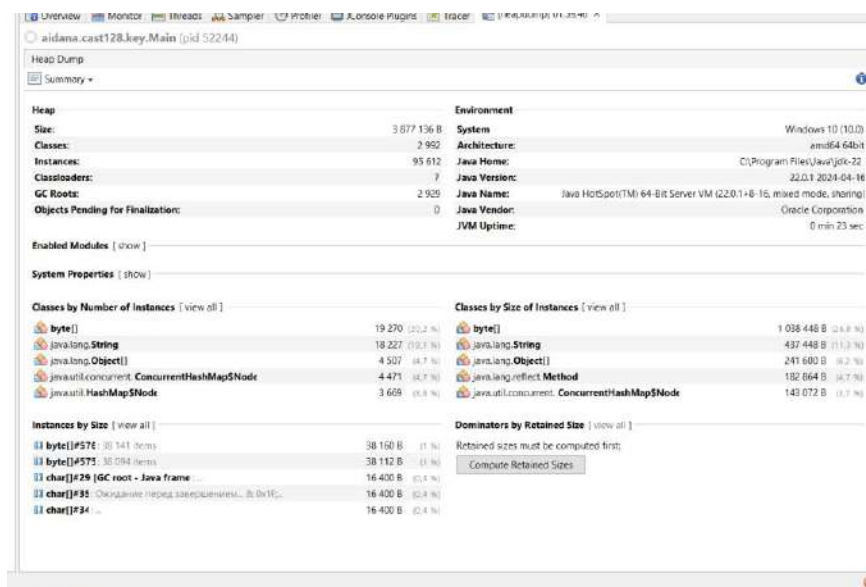
Екі блоктық шифрлардың алгоритімдеріне шолу жүргізу арқылы келесі ерекшеліктер алынды:

Ерекшеліктер	CAST-128	Kuznyechik
Блок өлшемі	64 бит	128 бит
Кілттің өлшемі	өзгереді (40-128 бит)	бекітілген (256 бит)
Шифрлау раундтарының саны	раундтар саны - 12-16	раундтар саны - 10
Құрылымы	Фейстель желісінің	Substitution-Permutation Network (SPN)
S-box дизайны	бірнеше раундқа тәуелді S-блоктары	қауіпсіздікті қамтамасыз ету үшін оңтайландырылған бір бекітілген S-блоктары

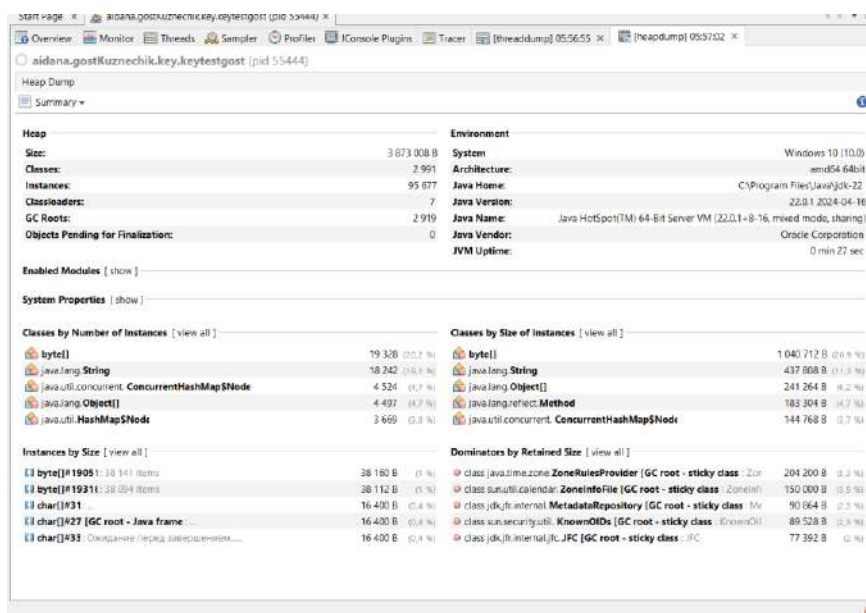
Кесте 1. CAST-128 және Kuznyechik блоктық шифрларының блок өлшемі, кілттің өлшемі, шифрлау раундтарының саны, құрылымы, S-box дизайны бойынша салыстырмалы сипаттамасы.

VisualVM көмегімен блоктық шифрлауды жүзеге асыруды талдау

VisualVM-Java программаларын бақылауға, ақаулықтарды жоюға және оңтайландыруға арналған қуатты, жан-жақты құрал. Бірнеше JDK пәрмен жолы құралдарын бір графикалық интерфейске біріктіру арқылы VisualVM әзірлеушілерге программа өнімділігін талдаудың, қиындықтарды анықтаудың және жұмыс уақытында ақауларды жоюдың интуитивті түсінікті құралы болып келеді.



Сурет 1. CAST-128 кілт генерациясының VisualVM программасындағы көрінісі.



Сурет 2. Kuzneshik кілт генерациясының VisualVM программасындағы көрінісі.

VisualVM көмегімен CAST-128 және Kuzneshik Кілттерін генерациялау алгоритмдерін салыстыру нәтижесі алынды. Екі алгоритмде де кілттерді генерациялау функциялары қолданылады, бірақ олардың дизайн философиясы, ресурстарды пайдалану және криптографиялық күшті жақтары айтарлықтай ерекшеленеді. Төменде VisualVM көмегімен жүргізілген талдаулар негізінде егжей-тегжейлі салыстыру берілген.

Аспекттері	CAST-128 кілт генерациясы	Kuzneshik кілт генерациясы
Алгоритм түрі	Фейстель құрылымы бар жеңіл блоктық шифр.	SPN құрылымы бар заманауи блок шифры.

Аспектiлерi	CAST-128 кiлт генерациясы	Kuzneshik кiлт генерациясы
Жадты пайдалану	Тиiмдi үйiн көлемi ~12 МБ, онда byte[] және String нысандары басым	byte [] нысандары басым және жадтың жүктемесi сәл жоғары (~13 МБ үйiн).
CPU қолданылуы	Процессордың жүктелуi минималды (~0,0%), бұл операциялардың жеңiлдетiлгенiн көрсетедi (1-сурет).	Процессордың төмен жүктемесi (~40%), бұл операциялардағы үлкен есептеу жүктемесiн көрсетедi (2-сурет).
Ағын белсендiлiгi	13 белсендi ағын мен тұрақты ағын әрекетi; ағынның минималды уақыты (~43 мс).	Тұрақты жұмыс уақыты бар тұрақты ағын әрекетi (~50 мс).
Қоқыс жинау	кiлттердi жоспарлау кезiнде жадының тиiмдi басқарылуын, қоқыс жинаудың минималды белсендiлiгiнен көреміз.	үздіксіз орындалудың қамтамасыз етiлгенiн, деректердi жинау белсендiлiгiнің аздығынан көрiнедi.
Кiлт генерациясының күрделiлiгi	Модульдiк арифметика мен биттік амалдарды қолданатын салыстырмалы түрдегi қарапайым кiлт генерациясы.	Бiрнеше S-блоктарын, сызықтық түрлендiрулердi және модульдiк математиканы қамтитын күрделi кiлт генерациясы.
Криптотөзiмдiлiк	Ескiрген жүйелер үшiн жеткiлiктi, бiрақ блоктың кiшiрек өлшемеiне байланысты қазiргi стандарттар бойынша төмен (64 бит).	Блоктың үлкендiгi(128 бит) және заманауи дизайн принциптерi болғандықтан қауiпсiздiгi жоғары

Кесте 2. CAST-128 және Kuzneshik кiлт генерациясын VisualVM программасы арқылы келесi аспектiлердi салыстыру кестесi: алгоритм түрi, жадты пайдалану, CPU қолданылуы, ағын белсендiлiгi, қоқыс жинау, кiлт генерациясының күрделiлiгi, криптотөзiмдiлiк.

Қорытынды

Бұл зерттеу криптографиялық дизайнның өнiмдiлiк пен қауiпсiздiкке қалай әсер ететiнiн көрсетедi. Feistel құрылымы бар CAST-128 процессорды (~0%) және жадты (~12 МБ үйiндi) аз пайдаланудың арқасында ескiрген жүйелер үшiн тиiмдi, бiрақ оның 64 биттік блок өлшемеi мен айнымалы кiлт ұзындығы заманауи шабуылдарға төзiмдiлiктi шектейдi. Kuzneshik (ГОСТ Р 34.12-2015), оның SPN құрылымы, 128 биттік блоктары және 256 биттік кiлттерi бар, қауiпсiздiктiң жоғары деңгейiн қамтамасыз етедi, бiрақ есептеу шығындарын (процессор ресурстарының ~40%) және жадты көбiрек пайдалануды (~13 МБ үйiндi) қажет етедi. Visualvm профилi cast-128-дiң төмен қауiптi тапсырмаларға жарамдылығын және kuzneshik-тiң жоғары

қауіпсіздік қосымшаларына сенімділігін көрсете отырып, осыныларды растайды. Болашақта kuznychik өнімділігін оңтайландыру үшін гибриді іске асыруды немесе аппараттық жеделдетуді зерттеуге болады.

Қолданылған әдебиеттер тізімі

1. RFC 2144: The CAST-128 Encryption Algorithm // Internet Engineering Task Force (IETF). – 1997. – URL: <https://www.rfc-editor.org/rfc/rfc2144.txt>.
2. RFC 7801: GOST R 34.12-2015 Block Cipher "Kuznyechik" // Internet Engineering Task Force (IETF). – 2016. – URL: <https://www.rfc-editor.org/rfc/rfc7801.html>.
3. ISO/IEC 18033-3 Standard: Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers // International Organization for Standardization (ISO). – Geneva, 2005.
4. Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm // IOSR Journal of Engineering, Vol.6 Issue6, June 2016. – URL: [https://www.iosrjen.org/Papers/vol6_issue6%20\(part-1\)/A066010107.pdf](https://www.iosrjen.org/Papers/vol6_issue6%20(part-1)/A066010107.pdf) (дата обращения: 30.03.2025).
5. Profiling JVM Applications Remotely Using VisualVM // ITNEXT, June 2024. – URL: <https://itnext.io/profiling-jvm-applications-remotely-using-visualvm-c0df9816aabf> (дата обращения: 30.03.2025).

ӘӨЖ 004.056.5

ЖЕРГІЛІКТІ ЖЕЛІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТЕТІН НЕГІЗГІ ПАРАМЕТРЛЕР

Акимбекова Дильназ Маратовна, Каиржанова Дильназ Жалғасқызы

akimbekovadilnaz@mail.ru, dikairzhanova@gmail.com

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Қазіргі заманғы желілер кибершабуылдарға жиі ұшырайды, олардың ішінде рұқсатсыз қол жеткізу, «қызмет көрсетуден бас тарту» (DoS/DDoS) шабуылдары және деректерді ұстап қалу сияқты қауіптер бар. Желілік құрылғылардың қауіпсіздігін қамтамасыз ету ақпаратты қорғаудың және ықтимал шабуылдардың алдын алудың негізгі шараларының бірі болып табылады.

Үйлердегі немесе үй желілеріндегі жергілікті желілерге (LAN) ерекше назар аударған жөн. Үй желілері – бұл жергілікті желілердің бір түрі; олар интернетке қосылған құрылғылардың кең және алуан түрін қамтуы мүмкін және оларды басқару оңай, сенімді және қауіпсіз болуы керек, әсіресе олардың иелері көбінесе техникалық дағдылары жоқ пайдаланушылар болғандықтан [1].

Көптеген жылдар бұрын үй желісі сымсыз желіге қосылған бірнеше ноутбуктан тұрған. Бүгінгі таңда оған смартфондар, сымсыз принтерлер, термостаттар, дыбыс датчиктері, түтін датчиктері, шамдар, камералар, теледидарлар, аудио жүйелері, ақылды динамиктер, тоңазытқыштар және тағы басқалар кіруі мүмкін. "Заттар интернеті" (IoT, Internet of Things) деп аталатын интернетке үйлесімді құрылғылардың көбеюі кез-келген электрониканы, соның ішінде әртүрлі сенсорларды желіге қосуға мүмкіндік береді. Қосылған құрылғылардың бұл