"JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN" JURNALI
VOLUME 04, ISSUE 03, 2026. MARCH
ResearchBib Impact Factor: 9.654/2024 ISSN 2992-8869

MOLIYAVIY AXBOROT TIZIMLARIDA KRIPTOGRAFIK HIMOYA MEXANIZMLARINING SAMARADORLIGI VA KALIT GENERATSIYASI MUAMMOLARI

Salamat Mirzatayev,
Ilmiy rahbar, professor v.b. Qoraqalpoq davlat universiteti,
Timur Jorabekov,
Qoraqalpoq davlat universiteti, katta o'qituvchi
Omirbayev Baxram Jangabayevich,
Qoraqalpoq davlat universiteti, "Kompyuter tizimlari va ularning dasturiy ta'minoti" 1-kurs magistranti

Annotatsiya: *Maqolada moliyaviy axborot tizimlarida simmetrik kriptografik algoritmlar, xususan AES va ChaCha20-Poly1305, samaradorligi va ularning turli platformalardagi ishlash ko'rsatkichlari tahlil qilinadi. Shuningdek, kalit generatsiyasi, psevdo-tasodifiy sonlar generatorlari va kalitlarni boshqarish masalalari ko'rib chiqilgan. Tadqiqot natijalari AES algoritmining apparat tezlashtirishda yuqori samaradorligini, ChaCha20-Poly1305 esa resurs cheklangan muhitlarda ustunligini ko'rsatadi. Kalit sifatining barqarorligi va yetarli entropiya darajasi tizim xavfsizligining asosiy omillari sifatida ta'kidlangan.*

Kalit so'zlar: *kriptografiya; AES; ChaCha20-Poly1305; simmetrik shifrlash; kalit generatsiyasi; psevdo-tasodifiy sonlar generatori; kalit boshqaruvi; moliyaviy axborot tizimlari xavfsizligi*

Abstract: *This paper analyzes the performance of symmetric cryptographic algorithms, particularly AES and ChaCha20-Poly1305, in financial information systems across different computational platforms. Key generation, pseudo-random number generators, and key management practices are also examined. Results show AES performs best with hardware acceleration, while ChaCha20-Poly1305 excels in resource-constrained environments. Key quality and sufficient entropy are highlighted as critical factors for system security.*

Keywords: *cryptography; AES; ChaCha20-Poly1305; symmetric encryption; key generation; pseudo-random number generator; key management; financial information system security*

Аннотация: *В статье анализируется эффективность симметричных криптографических алгоритмов, в частности AES и ChaCha20-Poly1305, в финансовых информационных системах на различных вычислительных платформах. Рассматриваются генерация ключей, генераторы псевдослучайных чисел и управление ключами. Результаты показывают, что AES обеспечивает наилучшую производительность при аппаратном ускорении, тогда как ChaCha20-Poly1305 эффективен в ресурсно-ограниченных средах. Качество ключей и достаточная энтропия выделяются как критические факторы безопасности системы.*

Ключевые слова: *криптография; AES; ChaCha20-Poly1305; симметричное шифрование; генерация ключей; генератор псевдослучайных чисел; управление ключами; безопасность финансовых информационных систем*

Kirish

Raqamli iqtisodiyot sharoitida bank tizimlari, elektron to‘lov platformalari hamda moliyaviy xizmatlar infratuzilmasida axborot xavfsizligini ta’minlash ustuvor vazifaga aylandi. Ushbu tizimlarda qayta ishlanadigan moliyaviy axborotlar, jumladan mijozlarga oid shaxsiy ma’lumotlar, to‘lov rekvizitlari, bank kartalari bilan bog‘liq axborotlar hamda tranzaksiya tafsilotlari yuqori darajadagi maxfiylik, yaxlitlik va ishonchlilikni talab qiladi. Mazkur talablarning bajarilmasligi moliyaviy yo‘qotishlar, axborot sizib chiqishi va tizimlarga bo‘lgan ishonchning pasayishiga olib kelishi mumkin.

Moliyaviy tizimlarda asosiy simmetrik shifrlash standarti sifatida AES algoritmi keng qo‘llaniladi [1], [5] hamda xalqaro to‘lov xavfsizligi talablariga muvofiq moliyaviy ma’lumotlarni himoyalashning asosiy kriptografik mexanizmi sifatida qaraladi. ISO 9564-1 standarti doirasida joriy etilgan Format 4 PIN-blok kuchli shifrlash algoritmlarini qo‘llashga mo‘ljallangan bo‘lib, AES asosida PIN-ma’lumotlarni zamonaviy talablarga mos ravishda himoyalash imkonini beradi [2], [5]. Zamonaviy tarmoq aloqalarini himoyalashda esa autentifikatsiyalangan shifrlash mexanizmlari qo‘llanilib, ChaCha20–Poly1305 algoritmi yuqori samaradorlik va kriptografik barqarorlikni ta’minlovchi yechim sifatida e’tirof etiladi [3]. Shu bilan birga, kriptografik mexanizmlarning ishonchliligi bevosita kalitlarning sifatiga bog‘liq. Amaliyot shuni ko‘rsatadiki, algoritm matematik jihatdan mustahkam bo‘lsa ham, kalitlarni generatsiya qilish jarayonida entropiya

yetishmovchiligi sababli tizim xavfsizligi zaiflashishi mumkin. Kalitlarni yaratish va boshqarish tamoyillari xalqaro tavsiyalarda batafsil belgilangan bo‘lib [4], kuchli algoritm bilan bir qatorda ishonchli kalit boshqaruvi tizimi zarurligi alohida ta’kidlanadi.

Moliyaviy axborot tizimlarida axborotni himoyalash masalasi kriptografik himoya vositalariga bevosita bog‘liq bo‘lib, bunda shifrlash algoritmlari va ularni boshqaruvchi kriptografik kalitlar muhim ahamiyat kasb etadi. Kalitlarning sifati, ularning bashorat qilib bo‘lmasligi hamda yetarli entropiyaga ega bo‘lishi kriptografik tizimning barqarorligi va ishonchliligini belgilovchi asosiy omillar hisoblanadi. Shu bois moliyaviy axborot tizimlari uchun kalitlar generatorining kriptografik barqarorligi, yuqori entropiya darajasi va platformalararo moslashuvchanligini ta’minlash dolzarb ilmiy-amaliy muammo bo‘lib, mazkur tadqiqot ishining maqsadi ushbu tizimlar talablaridan kelib chiqib samarali va ishonchli kalitlar generatorini ishlab chiqishning nazariy hamda amaliy asoslarini belgilashdan iborat.

Mavzuga oid adabiyotlar sharhi

Kriptografik himoya vositalari, xususan simmetrik shifrlash algoritmlari va kriptografik kalitlarni boshqarish masalalari ko‘plab xorijiy olimlarning ilmiy tadqiqotlarida keng yoritilgan. Advanced Encryption Standard (AES) algoritmining nazariy asoslari va amaliy qo‘llanilishi National Institute of Standards and Technology tomonidan ishlab chiqilgan FIPS 197 standartida batafsil bayon etilgan bo‘lib, u zamonaviy axborot va moliyaviy tizimlarda asosiy shifrlash standarti sifatida e’tirof etiladi.

AES algoritmining tuzilishi, xavfsizlik xususiyatlari va ishlash samaradorligi Menezes va Vanstone tomonidan yozilgan “Handbook of Applied Cryptography”, shuningdek Ferguson va Schneierning “Practical Cryptography” asarlarida ilmiy jihatdan asoslab berilgan. Ushbu manbalarda kriptografik kalitlarning sifati, ularning uzunligi va tasodifiyligi butun shifrlash tizimi xavfsizligiga bevosita ta’sir qilishi ta’kidlangan.

Kriptografik algoritmlardagi xavfsizlik muammolari Murtaza Nikzad va Kerem Atas tomonidan olib borilgan ilmiy tadqiqotlarda yoritilgan bo‘lib, unda RSA algoritmida kalitlar generatsiyasi jarayonidagi kamchiliklar va ularning amaliy xavf-xatarlari tahlil qilingan [7]. Shuningdek, Saydahd, Muhammed va Hassanlarning

ilmiy ishlarida AES hamda ChaCha20 algoritmlarining xavfsizlik va unumdorlik jihatlari qiyosiy tahlil qilingan [6].

Kalitlarni boshqarish va ularning hayotiy sikliga oid masalalar NIST Special Publication 800-57 tavsiyalarida keng yoritilgan bo'lib, ushbu hujjatda yuqori entropiyaga ega, ishonchli va barqaror kalitlar generatorlarini qo'llash zarurligi asoslab berilgan. To'lov tizimlari uchun kriptografik algoritmlar va kalitlarni boshqarish bo'yicha amaliy tavsiyalar esa European Payments Council tomonidan ishlab chiqilgan qo'llanmalarda keltirilgan [5]. Shu bilan birga, mavjud adabiyotlarda moliyaviy axborot tizimlari talablariga mos, yuqori tezlikni ta'minlovchi va platformalararo ishlay oladigan kalitlar generatorlarini ishlab chiqish masalalari yetarli darajada kompleks va tizimli yoritilmaganligini qayd etish mumkin. Bu holat mazkur yo'nalishda qo'shimcha ilmiy izlanishlar olib borish zaruratini ko'rsatadi.

Tadqiqot metodologiyasi

Mazkur ish nazariy-tahliliy xarakterga ega bo'lib, moliyaviy axborot tizimlarida qo'llaniladigan kriptografik mexanizmlar va kalitlar generatsiyasi masalalari mavjud ilmiy manbalar, xalqaro standartlar (NIST SP 800-57, 800-90A, 800-90B) va ochiq texnik hujjatlar asosida tahlil qilindi. Tadqiqotda analiz, sintez, induksiya va deduksiya usullari yordamida simmetrik algoritmlar (AES, ChaCha20-Poly1305) va ularning kalit xususiyatlari sistematik tarzda o'rganildi. Shuningdek, entropiya manbalari, zaif kalitlar va real hayot xavfsizlik hodisalari nazariy jihatdan baholandi. Ushbu metodologiya moliyaviy axborot tizimlarida kriptografik xavfsizlikni tizimli va ilmiy asoslangan tarzda tadqiq etishga yo'naltirilgan.

Tahlil va natijalar

Moliyaviy axborot tizimlarida (MAT) qo'llaniladigan kriptografik algoritmlar amaliy samaradorlik, normativ moslik va xavfsizlik zaxirasi mezonlari asosida tahlil qilindi. Tahlillar shuni ko'rsatadiki, AES (Advanced Encryption Standard) algoritmi bank kartalari ma'lumotlari, tranzaksiya axboroti va PIN-bloklarni himoyalashda asosiy simmetrik shifrlash mexanizmi sifatida keng qo'llaniladi. AES 2001-yilda NIST tomonidan FIPS 197 standarti sifatida tasdiqlangan bo'lib, 128-bit blok va 128/192/256-bit kalit o'lchamlarini qo'llab-quvvatlaydi [1]. PCI DSS talablari ham to'lov kartalari ma'lumotlarini himoyalashda kuchli kriptografiya, xususan AES dan foydalanishni majburiy deb belgilaydi [12].

Nazariy baholashlarga ko‘ra, AES-128 algoritmi uchun 2^{128} o‘lchamdagi kalit fazosini oddiy bruteforce usuli bilan to‘liq tekshirish amaliy jihatdan imkonsiz darajada murakkab bo‘lib, bu uning yuqori kriptobardoshliligini ko‘rsatadi [13]. Zamonaviy hisoblash texnologiyalari rivojlanayotganiga qaramay, mavjud va kutilayotgan hisoblash quvvatlari sharoitida bunday hujumni amalga oshirish real tahdid sifatida qaralmaydi. Bundan tashqari, apparat tezlashtirish texnologiyalari, xususan AES-NI ko‘rsatmalaridan foydalanilganda, AES algoritmi yuqori o‘tkazuvchanlik va samaradorlikni ta’minlaydi hamda optimallashtirilgan dasturiy realizatsiyalar bilan solishtirganda bir necha barobar tez ishlashi tajribaviy natijalar bilan tasdiqlangan [14].

Zamonaviy moliyaviy veb-xizmatlarda ma’lumot uzatish xavfsizligi asosan RFC 8446 bilan belgilangan TLS 1.3 protokoli orqali ta’minlanadi. Mazkur standartda faqat autentifikatsiyalangan shifrlash (AEAD) rejimlaridan foydalanish nazarda tutilgan bo‘lib, AES-GCM va ChaCha20-Poly1305 kabi shifrlash to‘plamlari qo‘llab-quvvatlanadi [15]. AES algoritmi yuqori samaradorligi va keng apparat qo‘llab-quvvatlovi tufayli amaliy tizimlarda yetakchi o‘rin tutadi, biroq maxsus apparat tezlashtirish mavjud bo‘lmagan muhitlarda uning unumdorligi pasayishi mumkin. Shu sababli dasturiy realizatsiyada yuqori tezlik va vaqt bo‘yicha barqarorlikni ta’minlaydigan ChaCha20 algoritmi taklif etilgan [16]. ChaCha20 oqimli shifri va Poly1305 autentifikatsiya kodi kombinatsiyasi asosida qurilgan ChaCha20-Poly1305 AEAD sxemasi ma’lumotlarning maxfiyligi va yaxlitligini birgalikda kafolatlaydi hamda IETF protokollarida, jumladan TLS 1.3 da qo‘llanadi [3]. Ushbu mexanizmlar moliyaviy portallar va API xizmatlarida uzatilayotgan ma’lumotlarning kriptografik jihatdan ishonchli himoyalanishini ta’minlaydi.

Shuningdek, ISO 9564-1 Format 4 PIN-blok kuchli blokli shifrlash algoritmlarini qo‘llash uchun ishlab chiqilgan bo‘lib, AES ni qo‘llab-quvvatlaydigan zamonaviy format sifatida tavsiflanadi [8]. Triple DES (3DES) ayrim moliyaviy tizimlarda uchrasa-da, xavfsizlik va ishlash samaradorligi nuqtai nazaridan AES bilan solishtirganda eskirayotgan algoritm sifatida baholanadi. Tadqiqot natijalari shuni ko‘rsatadiki, AES algoritmi xavfsizlik va tezkorlik ko‘rsatkichlari bo‘yicha 3DES hamda RSA dan ustun hisoblanadi; xususan, 128-bitli AES kalitining kriptobardoshliligi taxminan 2600-bitli RSA kalitiga teng deb baholanadi. Shu bilan birga, DES eng kam energiya sarflasa-da, bruteforce hujumlariga nisbatan juda zaif bo‘lib, qisqa vaqt ichida buzilishi mumkinligi aniqlangan [9]. Mazkur natijalar AES

ning zamonaviy moliyaviy axborot tizimlarida asosiy shifrlash standarti sifatida qo‘llanilishining ilmiy asosga ega ekanligini tasdiqlaydi.

Tahlil natijalari umumlashtirilgan holda 1-jadvalda keltirilgan.

Algoritm	Blok / kalit o‘lchami	Qo‘llanilish sohasi	Xavfsizlik holati	Standart / manba
AES-128/256	128-bit blok; 128/256-bit kalit	Ma’lumotlarni saqlash, PIN-bloklar, tranzaksiyalar	Amaliy buzilishlar aniqlanmagan	FIPS 197 [1], PCI DSS [2]
3DES (TDEA)	64-bit blok; 112/168-bit kalit	Mavjud (meros) tizimlar	Eskirayotgan, samaradorligi past	PCI PIN Requirements [6]
ChaCha20-Poly1305	256-bit kalit (AEAD)	TLS 1.3, API va veb-xizmatlar	Amaliy buzilishlar aniqlanmagan	RFC 8446 [4]

1-jadval. Moliyaviy axborot tizimlarida qo‘llaniladigan asosiy shifrlash algoritmlarining taqqosiy tavsifi

Jadval natijalari shuni ko‘rsatadiki, moliyaviy axborot tizimlarida AES algoritmi normativ hujjatlar bilan mustahkamlangan, amaliy jihatdan sinovdan o‘tgan va apparat tezlashtirish imkoniyatlariga ega bo‘lgan asosiy kriptografik standart hisoblanadi. ChaCha20-Poly1305 esa xavfsiz tarmoq aloqasi uchun yuqori samaradorlik va moslashuvchanlikni ta’minlaydi. 3DES esa asosan tarixiy va muvofiqlik sabablari bilan ayrim tizimlarda saqlanib qolgan.

Quyidagi 2-jadvalda moliyaviy axborot tizimlarida (MAT), jumladan bank tizimlari, to‘lov infratuzilmalari hamda moliyaviy ma’lumotlarni uzatish va saqlash jarayonlarida real amaliyotda qo‘llaniladigan shifrlash algoritmlarining asosiy texnik ko‘rsatkichlari umumlashtirilgan. MAT standartlarida qo‘llanilmaydigan yoki tavsiya etilmagan algoritmlar jadvalga kiritilmadi.

Shifrlash algoritmi	Blok / kalit o‘lchami	Dasturiy ta’minotdagi unumdorlik (HW yordamida)	Apparat darajasidagi unumdorlik (FPGA/ASIC)	Xavfsizlik darajasi (taxminiy)	Asosiy tavsiflar
AES-128	128-bit blok / 128-bit kalit	1–15 Gbps (AES-NI, ARM Crypto)	10–50 Gbps	To‘liq raundlar uchun amaliy buzilishlar aniqlanmagan; keng	Jahon standarti; GCM, CBC, CTR kabi ko‘plab

				kriptotahlildan o'tgan	rejimlarni qo'llab-quvvatlaydi
AES-256	128-bit blok / 256-bit kalit	0.8–13 Gbps	10–40 Gbps	AES-128 ga nisbatan yuqoriroq kriptografik zaxira	Uzoq muddatli va post-kvant xavfsizlik uchun tavsiya etiladi
3DES	64-bit blok / 168-bit kalit (3-kalitli)	0.3–3 Gbps	2–10 Gbps	Zamonaviy talablarga nisbatan zaiflashib bormoqda	NIST tomonidan eskirgan deb e'lon qilingan; AES ga qaraganda sekin
ChaCha20	Oqimli shifr / 256-bit kalit (512-bit ichki holat)	1–12 Gbps (CPU ga bog'liq)	FPGA da kam qo'llanadi	Amaliy buzilishlar aniqlanmagan	Ko'pincha Poly1305 bilan birga (AEAD) ishlatiladi

2-jadval. Moliyaviy axborot tizimlarida qo'llaniladigan shifrlash algoritmlarining taqqosiy ko'rsatkichlari

Jadval va tahliliy ma'lumotlar Rahoul Ganesh va hammualliflarining *International Journal of Information Security* jurnalida (2025) chop etilgan "A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges" nomli maqolasidagi 14-jadval asosida umumlashtirildi va ushbu tizimlar uchun dolzarb bo'lgan qismi tanlab olinib, ilmiy bayon talablariga muvofiq qayta ishlangan [10].

Tarmoq muhitida kriptografik kalitlarning ishonchliligi nafaqat algoritm mustahkamligiga, balki kalitlarni to'g'ri generatsiya qilish va boshqarish jarayoniga ham bevosita bog'liq. Amaliy tadqiqot natijalari internet infratuzilmasida takrorlanuvchi va zaif kalitlar keng tarqalganini ko'rsatgan. Keng ko'lamli

skanerlash asosida TLS xostlarining 7 770 232 tasi (61%) va SSH xostlarining 6 642 222 tasi (65%) boshqa xostlar bilan bir xil ochiq kalitdan foydalangani aniqlangan [11]. Ayrim holatlarda bu umumiy hosting muhiti yoki bir tashkilotga tegishli sertifikatlar bilan izohlangan bo‘lsa-da, muhim qismi kalit generatsiyasi jarayonidagi muammolar bilan bog‘liq bo‘lgan. Xususan, past entropiya sharoitida kalit yaratish jiddiy xavfsizlik xatarini yuzaga keltirishi aniqlangan. Tadqiqot davomida 43 852 ta TLS xost (0,34%) kalit generatsiyasidagi yetarli tasodifiylik yo‘qligi sababli takrorlangan kalitlardan foydalangani qayd etilgan. SSH protokoli bo‘yicha esa 981 166 ta xost (9,60%) bir xil turdagi muammolar tufayli takroriy kalitlarga ega bo‘lgan [11]. Bunday zaifliklar turli ishlab chiqaruvchilarning tarmoq qurilmalarida aniqlangan bo‘lib, bu holat qurilma darajasidagi tizimli muammoni ko‘rsatadi.

Zaif kriptografik kalitlar. Kriptografik kalitlar raqamli aloqalarni himoyalashda, ma’lumotlarning maxfiyligi, butunligi va autentifikatsiyasini ta’minlashda hal qiluvchi ahamiyatga ega. Axborot tizimlarining, ayniqsa moliyaviy va kritik infratuzilmalarning xavfsizlik darajasi bevosita ushbu kalitlarning sifati va ulardan foydalanish amaliyotiga bog‘liq. Biroq kriptografik kalitlarni yaratish, boshqarish yoki tatbiq etish jarayonlaridagi kamchiliklar kuchli algoritmlardan foydalanilgan taqdirda ham butun tizim xavfsizligini zaiflashtirishi mumkin. Amaliy tajriba shuni ko‘rsatadiki, zaif kriptografik kalitlar asosiy axborot xavfsizligi xususiyatlarining buzilishiga olib keladi [20]: shifrlangan ma’lumotlarning ochilishi orqali maxfiylik yo‘qoladi, raqamli imzo va MAC qiymatlarining soxtalashtirilishi butunlikni izdan chiqaradi, hamda autentifikatsiya mexanizmlarining ishonchsizligi tizimga ruxsatsiz kirishlarga sabab bo‘ladi. Bunday zaifliklar nafaqat texnik, balki tashkiliy va iqtisodiy oqibatlarga ham ega bo‘lib, ma’lumotlarning sizib chiqishi, intellektual mulkning yo‘qotilishi, moliyaviy zararlar va tashkilot obro‘sining pasayishiga olib kelishi mumkin. Shu sababli kriptografik kalitlarning butun hayotiy siklini – yaratishdan tortib bekor qilishgacha bo‘lgan jarayonlarni to‘g‘ri va tizimli boshqarish axborot xavfsizligi strategiyasining ajralmas va markaziy elementi hisoblanadi.

Kriptografik tizimlarda kalit generatsiyasi jarayonidagi kamchiliklar hatto matematik jihatdan mustahkam algoritmlarning ham amaliy xavfsizligini izdan chiqarishi mumkin. Past entropiyali yoki bashorat qilinadigan psevdo-tasodifiy sonlar generatoridan foydalanish natijasida hosil qilingan kalitlar hujumchilar

tomonidan tiklanishi yoki oldindan aniqlanishi ehtimoli ortadi. 2021-yilda aniqlangan CVE-2021-41117 zaifligi kriptografik kalit juftligini yaratishda tasodifiylik mexanizmidagi nuqson kuchli algoritmlarni samarasiz holga keltirishi mumkinligini ko'rsatdi [17]. Natijada bashorat qilinadigan kalitlar yuzaga keladi, bu esa ruxsatsiz kirish va ma'lumotlar xavfsizligining buzilishiga olib keladi. Tarixiy tajriba bunday xavflar amaliyotda ham bir necha bor kuzatilganini ko'rsatadi. Jumladan, CVE-2008-0166 holatida Debian tizimlarida OpenSSL ning tasodifiy sonlar generatoridagi xato sabab kriptografik kalitlar oldindan taxmin qilinadigan tarzda yaratilgan [18]. Bu esa hujumchilarga kalitlarni brut-force usulida topish imkonini sezilarli darajada osonlashtirgan. Shuningdek, CVE-2017-15361 (ROCA) zaifligida ayrim qurilmalarda RSA kalitlarini generatsiya qilish jarayonidagi strukturaviy kamchilik tufayli ochiq kalit asosida yopiq kalitni hisoblab chiqish mumkin bo'lgan [19]. Muammo tub sonlarni yaratish algoritmidagi xususiyatlar bilan bog'liq bo'lib, ayrim apparat modullar va TPM chiplariga ta'sir ko'rsatgan.

Ushbu holatlar shuni ko'rsatadiki, kriptografik xavfsizlik faqat kuchli algoritm tanlash bilan ta'minlanmaydi. Tasodifiylik manbalarining sifati, kalit generatsiyasi jarayonining to'g'ri tashkil etilishi va implementatsiya ishonchliligi kamida algoritmning o'zi kabi muhim ahamiyatga ega.

Xulosa va takliflar

Tadqiqot shuni ko'rsatdiki, simmetrik kriptografik algoritmlarning xavfsizligi ularning matematik mustahkamligi, realizatsiya sifati va kalitlar sifatiga bog'liqdir. AES algoritmi apparat tezlashtirishni qo'llab-quvvatlaydigan server va ish stansiyalarida yuqori samaradorlikni ta'minlasa, ChaCha20 resurs cheklangan muhitlarda barqaror va past kechikish ko'rsatkichlariga ega.

Kriptografik tizim xavfsizligi kalitlar sifati va boshqaruv jarayoni bilan bevosita bog'liq. Shu sababli kalitlarni yaratishda yetarli entropiya va ishonchli tasodifiy sonlar generatorlaridan foydalanish, ularni saqlash, yangilash va tarqatish jarayonini xalqaro standartlarga muvofiq tashkil etish zarur. Gibrid kriptografiya yondashuvi simmetrik algoritmlarning tezligi va assimetrik algoritmlarning xavfsiz kalit almashish imkoniyatlarini birlashtirib, katta hajmdagi ma'lumotlarni samarali himoya qiladi, ayniqsa moliyaviy tizimlar va bulutli platformalarda. Takliflar:

- Kalitlar va parametrlarni yaratishda yetarli entropiya va ishonchli tasodifiy sonlar generatorlaridan foydalanish.

- Kalitlarni boshqarish siyosati asosida yaratish, saqlash, yangilash va audit qilish.
- Sertifikatlangan va sinovdan o‘tgan kriptografik modullar va kutubxonalarni qo‘llash.
- Xavfsizlik auditi va standartlarga muvofiqlikni muntazam baholash.
- Kalitlarni generatsiya qilish va boshqarish jarayonlarini xalqaro standartlarga muvofiq tashkil etish: NIST SP 800-57, ISO/IEC 19790, FIPS 140-3; tasodifiy sonlar generatsiyasi: NIST SP 800-90A, NIST SP 800-90B [21] [22].

Umuman olganda, kriptografik xavfsizlik faqat algoritm tanlash bilan cheklanmaydi; real xavfsizlik implementatsiya tafsilotlari, entropiya yig‘ish, kalitlarni audit qilish va boshqaruv mexanizmlari orqali ta’minlanadi.

Foydalanilgan adabiyotlar:

[1] National Institute of Standards and Technology. (2001). FIPS 197: Advanced Encryption Standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[2] Czempas, P. (2026, January 23). The challenging path to adopting the ISO Format 4 PIN block. Utimaco. https://utimaco.com/news/blog-posts/challenging-path-adopting-iso-format-4-pin-block

[3] Nir, Y., & Langley, A. (2018). ChaCha20 and Poly1305 for IETF protocols (RFC 8439). Internet Engineering Task Force. https://doi.org/10.17487/RFC8439

[4] National Institute of Standards and Technology. (2020). Recommendation for key management: Part 1 – General (NIST Special Publication 800-57 Part 1 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[5] European Payments Council. (2025). Guidelines on cryptographic algorithms usage and key management (Version 15.0, EPC342-08). https://www.epc-cep.eu

[6] Saydahd, S. J., Muhammed, R. K., Hassan, S. A., & Aladdin, A. M. (2024). A comparative performance evaluation of hybrid encryption techniques using ECC, RSA, AES, and ChaCha20 for secure data transmission. International Journal of Operations Research and Information Systems, 12(2). https://doi.org/10.53523/ijoirVol12I2ID598

[7] Nikzad, M., & Atas, K. (2025). When RSA fails: Exploiting prime selection vulnerabilities in public key cryptography. arXiv. https://doi.org/10.48550/arXiv.2512.22720

[8] PCI Security Standards Council. (2014). PIN Security Requirements, Version 2.0.

[9] Singh, A., Marwaha, M., Singh, B., & Singh, S. (2013). Comparative study of DES, 3DES, AES and RSA. International Journal of Computers & Technology, 9(3), 1162–1170.

[10] Ganesh, R., Khan, B. U. I., Khan, A. R., & Kamsin, A. B. (2025). A panoramic survey of the advanced encryption standard: From architecture to security analysis, key management, real-world applications, and post-quantum challenges. International Journal of Information Security, 24, 216. https://doi.org/10.1007/s10207-025-01116-x

[11] Heninger, N., Durumeric, Z., Wustrow, E., & Halderman, J. A. (2012). Mining your Ps and Qs: Detection of widespread weak keys in network devices. In Proceedings of the 21st USENIX Security Symposium (pp. 205–220). USENIX Association.

[12] PCI Security Standards Council. (2022). *PCI DSS v4.0: Payment Card Industry Data Security Standard.*

[13] Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg.

[14] Boneh, D., & Shoup, V. (2023). A Graduate Course in Applied Cryptography (Version 0.6, p. 121). Stanford University.

[15] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

[16] Bernstein, D. J. (2008). ChaCha, a variant of Salsa20. Workshop Record of SASC 2008. http://cr.yp.to/chacha/chacha-20080120.pdf

[17] GitHub Security Lab. (2021). GHSL-2021-1012: Poor random number generation in keypair (CVE-2021-41117). https://securitylab.github.com/advisories/GHSL-2021-1012-keypair/

[18] Deepak Shanker. (2017, October 17). ROCA: Vulnerable RSA key generation (CVE-2017-15361). Qualys. https://threatprotect.qualys.com/2017/10/17/roca-vulnerable-rsa-key-generation-cve-2017-15361/

[19] CVEDetails. (n.d.). CVE-2008-0166: OpenSSL on Debian predictable random number generator weakens cryptographic key security. https://www.cvedetails.com/cve/CVE-2008-0166/

[20] Aqtive Guard. (n.d.). Weak cryptography keys. https://docs.aqtiveguard.com/kb-articles/weak-cryptography-keys/

[21] Barker, E., & Kelsey, J. (2015). Recommendation for random number generation using deterministic random bit generators (NIST SP 800-90A Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90Ar1

[22] Turan, M. S., Barker, E., Kelsey, J., & McKay, K. (2018). Recommendation for the entropy sources used for random bit generation (NIST SP 800-90B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90B