TECH SCIENCE

ISSN 3030-3702

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

№ 3 (4) 2026

TECHSCIENCE.UZ

№ 3 (4)-2026

TEXNIKA FANLARINING DOLZARB MASALALARI

TOPICAL ISSUES OF TECHNICAL SCIENCES

TOSHKENT-2026

OAK Ro‘yxati
Mazkur jurnal O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi Rayosatining 2025-yil 8-maydagi 370-son qarori bilan texnika fanlari bo‘yicha ilmiy darajalar yuzasidan dissertatsiyalar asosiy natijalarini chop etish tavsiya etilgan ilmiy nashrlar ro‘yxatiga kiritilgan.

Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI elektron jurnali 15.09.2023-yilda 130343-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com

TEXNIKA FANLARINING DOLZARB MASALALARI
4-jild, 3 -son (Mart, 2026). – 133 bet.

MUNDARIJA

Maxarov Qodirbek, Ismatillayev Muzaffar
SUN'IY INTELLEKT TEXNOLOGIYALARI ASOSIDA TEZ YORDAM QO'NG'IROQLARINI QAYTA ISHLASH TIZIMI 5-11

Ergasheva Oxuna, Raximova Mehrbonu
TABIIY TILNI QAYTA ISHLASH YONDASHUVI BILAN INTEGRATSIYALASHGAN RAQAMLI TIBBIYOTNI MASOFADAN MONITORING QILISH DASTURINI ISHLAB CHIQISH 12-18

Jamalova Gulchexra
O'ZBEKISTON SOLIQ MA'MURIYATCHILIGINI TASHKIL ETISHDA SUN'IY INTELLEKTDAN FOYDALANISHNING TIZIMLI TAHLILI VA BOSHQARUV MEXANIZMLARINI TAKOMILLASHTIRISH 19-24

Arziqulov Husan
O'ZBEK TILI UCHUN SUN'IY INTELLEKT ASOSIDA UZLUKSIZ NUTQNI TANISH TIZIMINI YARATISH: KORPUS, AKUSTIK MODEL VA TIL MODELINI LOYIHALASH 25-31

Isakov Iskander, Xabibullaeva Dilnoza, Orazimbetov Temurbek
IDROKDAN AVTONOMIYAGACHA: KO'RISHGA YORDAM BERISH VA NEYRONLARNI TIKLASHDA MULTIMODAL SUN'IY INTELLEKTNING NARRATIV SHARHI (2020-2026) 32-44

Daliyev Sherzod
YER OSTI SIZOT SUVLARI DINAMIKASI O'ZGARISH JARAYONINI MATEMATIK MODELLASHTIRISH 45-52

Muradov Sirojiddin
EHTIMOLIY XAVFLARNI BAHOLASHDA FORSAYT TEXNOLOGIYASIDAN FOYDALANISH 53-62

Vasiyev Xayrullo, Abduolimova O'g'iloy
TO'QIMACHILIK MAHSULOTLARI SIFATINI XALQARO 4 BALLI BAHOLASH TIZIMI ASOSIDA BOSHQARISH METODIKASINI TAKOMILLASHTIRISH 63-68

Ergashxo'jayeva Sabohat, Shodmanov Jasur
ISHLAB CHIQARISH KORXONALARIDA CHANG HOSIL BO'LISH MANBALARI VA UNI BARTARAF ETISH USULLARI 69-75

Ismoilov Muxriddin, Rahimov Anvarjon, Asatov Shavkat, Norbayeva Malikaxon
EKSPERIMENTAL O'LCHASHLARDA STATISTIK TAHLIL VA XATOLIKLARNI KAMAYTIRISH USULLARINING TAHLILI 76-82

Jurayev O'tkirbek
BULUTLI HISOBLASH TIZIMLARIDA MA'LUMOTLARNI XAVFSIZ SHIFRLASHNING GIBRID KRIPTOGRAFIK ALGORITMI 83-91

Ismailov Ilxom, Raximov Rustamjon
MACHINE LEARNING YONDASHUVI YORDAMIDA
O‘ZBEKISTON VILOYATLARINI QISHLOQ XO‘JALIGI
KO‘RSATKICHLARI BO‘YICHA KLASTERLASH VA TASNIFLASH 92-100

Almataev Tojiboy, Zokirjonov Azizbek
EXPERIMENTAL INVESTIGATION ON LITHIUM-ION BATTERY AGING UNDER
UZBEKISTAN’S CLIMATE 101-114

Юнусалиев Эльмурод, Тошпулатов Ильхомжон
ИЗГОТОВЛЕНО ИЗ МЕСТНОЙ ДРЕВЕСИНЫ ПОДГОТОВЛЕННЫЕ
БАЛОЧНЫЕ КОНСТРУКЦИИ УСТОЙЧИВОСТЬ К РАСТЯЖЕНИЮ I 115-121

To‘xtaniyozova Muhayyo, To‘rayev Azizbek
O‘ZBEKISTON RESPUBLIKASIDA QURILISH MATERIALLARI SIFATI VA
XAVFSIZLIGINI TA’MINLASHNING INNOVATSION USULLARI: KOMPLEKS
TAHLIL VA METROLOGIK BAHOLASH 122-132

Texnika fanlarining dolzarb masalalari
Topical Issues of Technical Sciences
2026-yil | 4-jild | 3-son
ISSN (onlayn): 3030-3702

BULUTLI HISOBLASH TIZIMLARIDA MA'LUMOTLARNI XAVFSIZ SHIFRLASHNING GIBRID KRIPTOGRAFIK ALGORITMI

Jurayev O'tkirbek Murodullo o'g'li
Iqtisodiyot va pedagogika universiteti o'qituvchisi

Annotatsiya. Mazkur maqolada bulutli hisoblash tizimlarida ma'lumotlar xavfsizligini ta'minlash maqsadida gibrid kriptografik algoritm ishlab chiqish va uning samaradorligini baholash masalasi ko'rib chiqilgan.Tadqiqot davomida AES - 256 simmetrik shifrlash algoritmi hamda RSA - 2048 ochiq kalitli algoritmi kombinatsiyasi asosida yangi model taklif etildi [3].Tajriba natijalari algoritmning yuqori tezkorlik va xavfsizlik darajasini ta'minlashini ko'rsatdi [10].

Kalit so'zlar: Bulutli hisoblash, taqsimlangan hisoblash tizimlari,kriptografiya, zamonaviy kriptotizimlar, simmetrik shifrlash algoritmlari, assimetrik shifrlash algoritmlari, AES - 256,
RSA - 2048, gibrid kriptografik model, kalitlarni boshqarish mexanizmlari, ma'lumotlar maxfiyligi, ma'lumotlar yaxlitligi, axborot xavfsizligi, bulutli saqlash xavfsizligi, kalit almashinuvi protokollari, NIST standartlari, blokli shifrlash, ochiq kalitli kriptotizim, autentifikatsiya, raqamli imzo, kiberxavfsizlik[7].

HYBRID CRYPTOGRAPHIC ALGORITHM FOR SECURE DATA ENCRYPTION IN CLOUD COMPUTING SYSTEMS

Jurayev O'tkirbek
Lecturer at the University of Economics and Pedagogy

Annotation. This article examines the development of a hybrid cryptographic algorithm and the evaluation of its effectiveness to ensure data security in cloud computing systems. During the research, a new model was proposed based on the combination of the AES - 256 symmetric encryption algorithm and the RSA - 2048 public-key algorithm [3]. The experimental results demonstrated that the algorithm provides a high level of performance and security [10].

Keywords: Cloud computing, distributed computing systems, cryptography, modern cryptosystems, symmetric encryption algorithms, asymmetric encryption algorithms, AES - 256, RSA - 2048, hybrid cryptographic model, key management mechanisms, data confidentiality, data integrity, information security, cloud storage security, key exchange protocols, NIST standards, block cipher, public-key cryptosystem, authentication, digital signature, cybersecurity [7].

DOI: https://doi.org/10.47390/ts-v4i3y2026N11

Kirish. So'nggi o'n yillikda raqamli transformatsiya jarayonlari jadal sur'atlar bilan rivojlanib, bulutli hisoblash texnologiyalari global axborot infratuzilmasining ajralmas qismiga aylandi [5].Xususan, Amazon Web Services, Microsoft Azure va Google Cloud Platform kabi platformalar tashkilotlar va foydalanuvchilarga elastik, masshtablanuvchi hamda iqtisodiy jihatdan samarali IT - resurslardan foydalanish imkonini bermoqda.

Bulutli hisoblash (Cloud Computing) - bu hisoblash resurslari (serverlar, saqlash tizimlari, ma'lumotlar bazalari, tarmoqlar va dasturiy ta'minot)ni masofaviy ma'lumotlar markazlarida joylashtirish hamda ulardan internet orqali xizmat sifatida foydalanish modelidir [5].Ushbu modelning asosiy afzalliklari quyidagilardan iborat.Infratuzilma xarajatlarini

kamaytirish,Resurslarni tezkor masshtablash,Yuqori darajadagi mavjudlik (availability),Xizmat ko‘rsatish samaradorligi.Shu bilan birga, bulutli arxitekturaning o‘ziga xos xususiyati - ma’lumotlarning uchinchi tomon serverlarida saqlanishi - axborot xavfsizligi masalasini dolzarb muammoga aylantiradi [1].An’anaviy lokal tizimlardan farqli ravishda, bulutli muhitda ma’lumotlar foydalanuvchi nazoratidan tashqarida joylashadi.Bu esa quyidagi xavflarni yuzaga keltiradi.Ruxsatsiz kirish (unauthorized access).Ma’lumotlarni o‘zgartirish yoki buzish (data tampering).Kalitlarni o‘g‘irlash va kompрometatsiya qilish.Ichki tahdidlar (insider threats).Tarmoq orqali uzatishda ma’lumotlarni tutib olish (man-in-the-middle attacks).Axborot xavfsizligining asosiy tamoyillari - maxfiylik (confidentiality), yaxlitlik (integrity) va mavjudlik (availability) - bulutli tizimlarda alohida himoya mexanizmlarini talab etadi [1]. Ayniqsa, maxfiy ma’lumotlar (moliyaviy hujjatlar, shaxsiy ma’lumotlar, tijorat sirlariga oid axborotlar)ni himoyalashda kriptografik usullar asosiy vosita sifatida namoyon bo‘ladi.Zamonaviy kriptografiya simmetrik va assimetrik algoritmlarga asoslanadi [1]. Simmetrik algoritmlar yuqori tezkorlikni ta’minlasada, kalit almashinuvi muammosiga ega. Assimetrik algoritmlar esa kalit almashinuvini xavfsiz amalga oshiradi, biroq katta hajmdagi ma’lumotlar bilan ishlashda samaradorligi past bo‘ladi. Shu bois bulutli muhitda xavfsizlik va tezkorlik o‘rtasida optimal muvozanatni ta’minlaydigan gibrid kriptografik yondashuv zarur hisoblanadi [10].

Mazkur tadqiqot aynan shu muammoni hal etishga qaratilgan bo‘lib, bulutli hisoblash tizimlarida qo‘llash uchun samarali va amaliy jihatdan asoslangan gibrid kriptografik modelni ishlab chiqishni maqsad qiladi.Tadqiqot maqsadi bu bulutli hisoblash muhitida ma’lumotlar maxfiyligi va yaxlitligini ta’minlaydigan, tezkor hamda yuqori darajadagi kriptobardoshlikka ega gibrid kriptografik algoritmni ishlab chiqish va uning samaradorligini eksperimental baholash.Tadqiqot vazifalari esa tadqiqot maqsadiga erishish uchun quyidagi vazifalar belgilandi.Zamonaviy simmetrik (AES - 256) va assimetrik (RSA - 2048) algoritmlarning nazariy asoslarini tahlil qilish.Ularning hisoblash murakkabligi va xavfsizlik darajasini taqqoslash.Gibrid kriptografik model arxitekturasini ishlab chiqish.Taklif etilgan modelning ishlash algoritmini matematik jihatdan asoslash va eksperimental sinovlar asosida tezkorlik va xavfsizlik ko‘rsatkichlarini baholash va mavjud yechimlar bilan qiyosiy tahlil o‘tkazish.

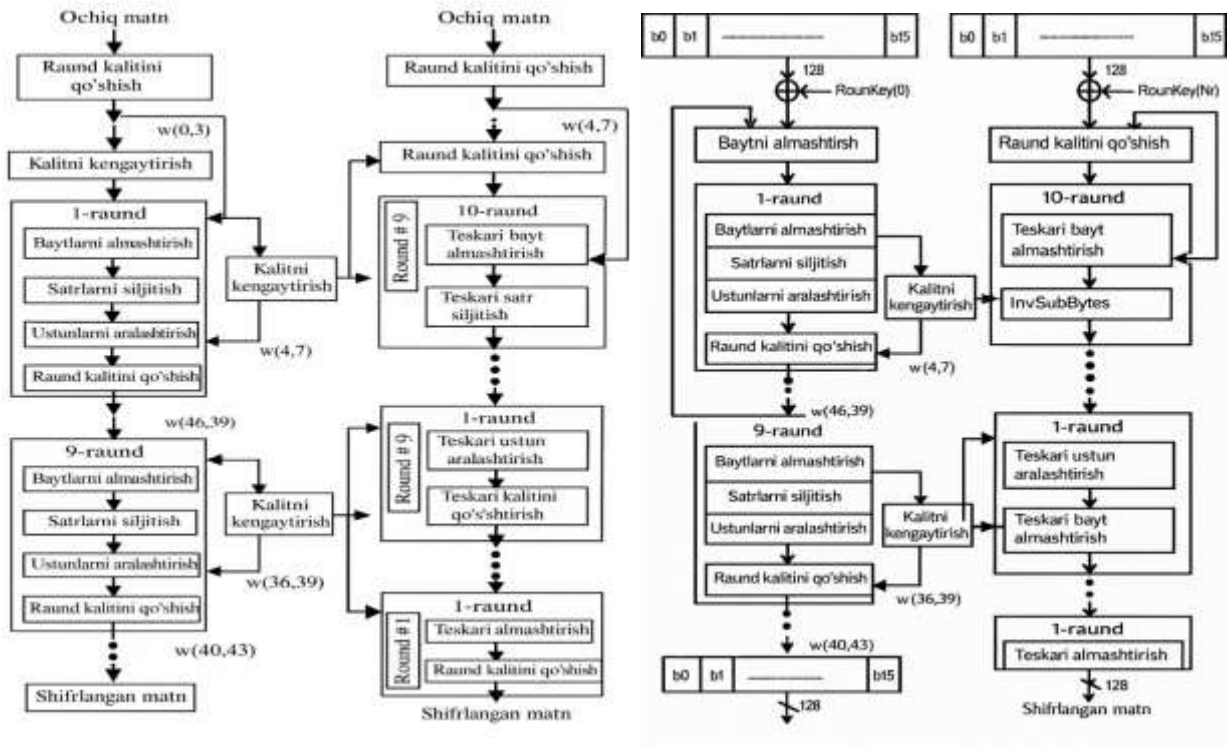
Adabiyotlar tahlili. Kriptografik algoritmlar axborot xavfsizligini ta’minlashning fundamental vositasi bo‘lib, ular matematik nazariya, sonlar nazariyasi va hisoblash murakkabligi konsepsiyalariga asoslanadi. Zamonaviy kriptotizimlar odatda ikki asosiy sinfga ajratiladi.Bular Simmetrik kriptografik algoritmlar va Assimetrik (ochiq kalitli) kriptografik algoritmlar.Ushbu ikki yondashuvning har biri ma’lum afzallik va cheklovlarga ega bo‘lib, amaliy tizimlarda ularning kombinatsiyalangan qo‘llanilishi samaraliroq natija beradi [1].

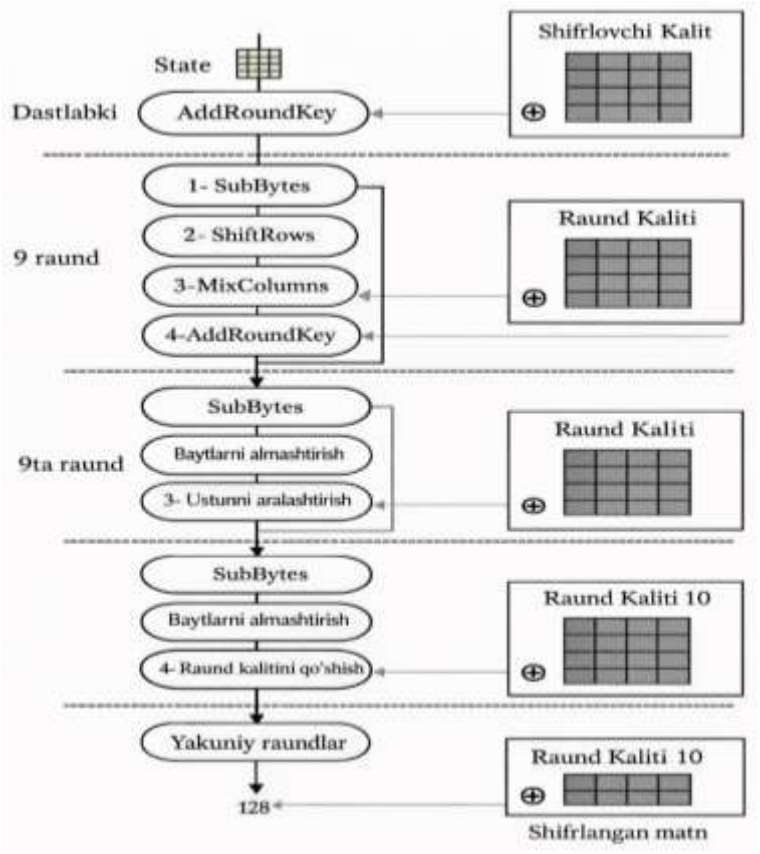
Simmetrik kriptografiyada shifrlash va deshifrlash jarayonlari bitta umumiy maxfiy kalit asosida amalga oshiriladi. Ushbu yondashuv yuqori tezkorlik va past hisoblash xarajatlari bilan ajralib turadi.Simmetrik algoritmlar orasida tarixan DES (Data Encryption Standard) keng qo‘llanilgan bo‘lsada, uning 56 - bitli kalit uzunligi zamonaviy hisoblash quvvatlari sharoitida yetarli darajada xavfsiz emas deb topilgan. Shu sababli DES o‘rnini zamonaviy standart - Advanced Encryption Standard (AES) egalladi [3]. AES blokli shifrlash algoritmi bo‘lib, 128 - bitli ma’lumot bloklari bilan ishlaydi. Kalit uzunligiga qarab 128, 192 va 256 bitli variantlari mavjud. AES - 256 versiyasi 14 ta iterativ raunddan iborat bo‘lib, har bir raund quyidagi transformatsiyalarni o‘z ichiga oladi.SubBytes - nolinear almashtirish. ShiftRows - satrlarni siklik siljitish [6].

MixColumns - ustunlarni aralashtirish (matritsali operatsiya). AddRoundKey - kalit bilan XOR amali. AES algoritmi AQSh Milliy Standartlar va texnologiyalar Instituti (NIST) tomonidan 2001 - yilda rasmiy standart sifatida qabul qilingan va bugungi kunda bank tizimlari, VPN, TLS protokollari hamda bulutli platformalarda keng qo‘llaniladi. Afzalliklari juda yuqori tezkorlik (hardware tezlatkichlar mavjud).Katta hajmdagi ma’lumotlar bilan ishlashga mos va kriptobardoshliligi yuqori.Global miqyosda standartlashtirilgan.

Kamchiliklari kalit almashinuvi muammosi (secure key distribution) kalit kompрometatsiya qilinsa, butun ma’lumot ochilishi mumkin (bulutli) muhitda kalitni xavfsiz saqlash murakkab. Bulutli hisoblash tizimlarida ma’lumotlar masofaviy serverlarda saqlanadi. Agar AES kaliti ruxsatsiz shaxs qo‘liga tushsa yoki noto‘g‘ri boshqarilsa, tizimning butun xavfsizlik modeli izdan chiqadi. Demak, simmetrik shifrlash tezkor bo‘lsada, kalit boshqaruvi masalasi uning asosiy zaif nuqtasidir [7].

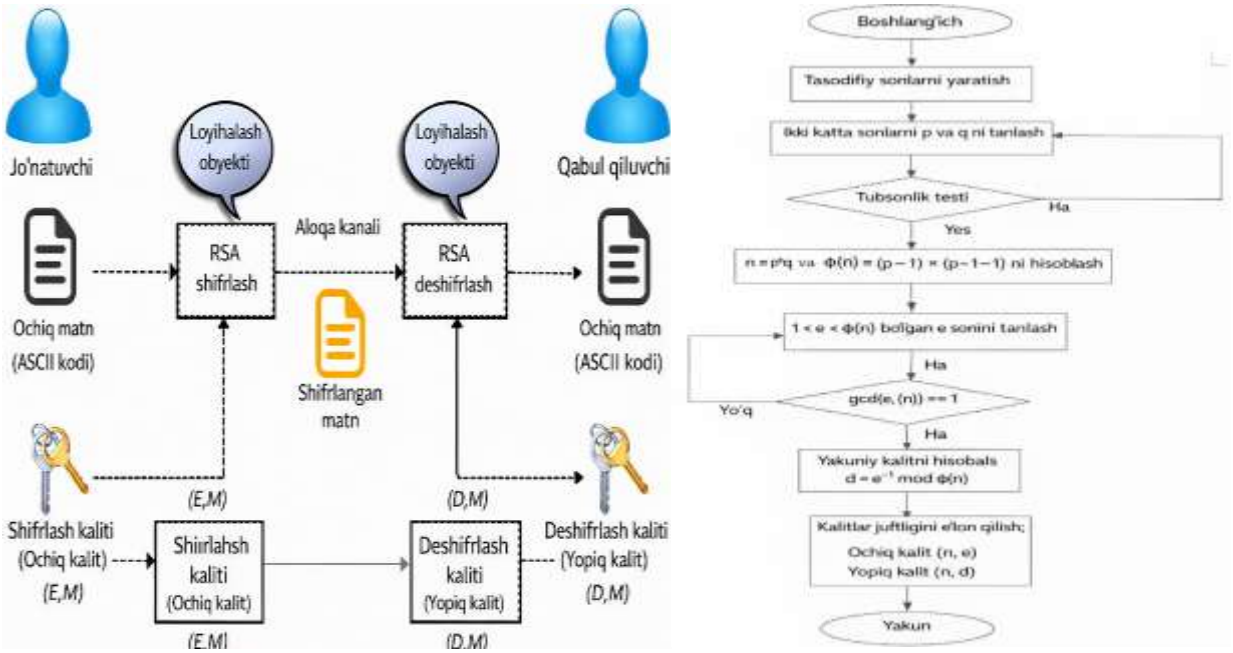
AES algoritmi





Assimetrik kriptografiyada ikkita turli kalit qo‘llaniladi: ochiq va yopiq kalit. Ushbu yondashuv kalit almashinuvi muammosini samarali hal qiladi va ochiq tarmoq muhitida xavfsiz aloqa o‘rnatish imkonini beradi.Assimetrik algoritmlarga misol sifatida RSA hamda Elliptic Curve Cryptography (ECC) keltiriladi.

RSA algoritmi



RSA algoritmi katta tub sonlarning faktorizatsiyasi hisoblash jihatdan murakkab ekanligiga asoslanadi. Uning matematik modeli quyidagicha ifodalanadi

$$C = \mathrm{AES}_{K_s}(M)$$

bu yerda $n = p \times q,$ bu yerda p va q - katta tub sonlar.

Afzalliklari xavfsiz kalit almashinuvi va autentifikatsiya va raqamli imzo imkoniyati [5], Ochiq tarmoqlarda qo‘llash uchun mos.Kamchiliklari hisoblash murakkabligi yuqori katta hajmdagi ma’lumotni shifrlashda sekin resurs sarfi kata muammo tahlili RSA algoritmini katta hajmli ma’lumotlarga qo‘llash tizim samaradorligini sezilarli darajada pasaytiradi. Bulutli muhitda bu server yuklamasining oshishi, kechikishlarning ko‘payishi, xizmat ko‘rsatish samaradorligining pasayishi kabi muammolarga olib keladi. Ilmiy muammo va mavjud bo‘shliq.Adabiyotlar tahlili shuni ko‘rsatadiki. Simmetrik algoritmlar tezkor, ammo kalit almashinuvi zaif.Assimetrik algoritmlar xavfsiz, ammo hisoblash jihatdan sekin.Bulutli hisoblash tizimlari esa bir vaqtning o‘zida yuqori tezkorlik, xavfsiz kalit boshqaruvi, masshtablanuvchanlik, resurs tejamkorlik talablarini qo‘ya di.Mavjud ilmiy ishlarda ko‘pincha faqat bir turdagi kriptografik mexanizmga urg‘u beriladi. Bu esa xavfsizlik va samaradorlik o‘rtasida optimal muvozanatni to‘liq ta’minlamaydi. Taklif etilayotgan yechim gibrid kriptografik yondashuv yuqoridagi muammolarni bartaraf etish uchun zamonaviy axborot xavfsizligi tizimlarida gibrid model qo‘llaniladi. Ushbu model quyidagicha ishlaydi: Ma’lumot AES yordamida tezkor shifrlanadi.AES kaliti RSA yordamida xavfsiz shifrlanadi. Shifrlangan ma’lumot va kalit bulut serverida saqlanadi.Tezkorlik saqlanadi.Kalit almashinuvi himoyalanadi.Hisoblash yuklamasi optimallashtiriladi.Bulutli muhit talablariga moslashuv ta’minlanadi [5].Literature Review bo‘limining yakuniy xulosasi. Tahlil shuni ko‘rsatadiki, bulutli hisoblash tizimlarida ma’lumotlar xavfsizligini ta’minlash uchun yagona kriptografik mexanizm yetarli emas. Simmetrik va assimetrik algoritmlarning kombinatsiyasi ya’ni gibrid model - xavfsizlik va samaradorlik o‘rtasidagi muvozanatni ta’minlovchi optimal yechim hisoblanadi. Mazkur tadqiqot aynan shu konseptual yondashuvni takomillashtirish va bulutli arxitektura sharoitida uning samaradorligini eksperimental jihatdan asoslashga qaratilgan.

TADQIQOT USULLARI. Taklif etilgan gibrid algoritm arxitekturasi. Taklif etilayotgan gibrid kriptografik model bulutli hisoblash muhitida ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash maqsadida ishlab chiqilgan [10].Model simmetrik va assimetrik kriptografiyaning ustun jihatlarini birlashtirishga asoslanadi.Arxitektura quyidagi asosiy komponentlardan iborat.Foydalanuvchi interfeysi (Client Side Module). Simmetrik shifrlash moduli (AES - 256 Engine). Assimetrik kalit boshqaruv moduli (RSA Module). Bulutli saqlash muhiti (Cloud Storage Layer). Jarayon asosiy bosqichda amalga oshiriladi.Ma’lumotni tayyorlash. Foydalanuvchi ma’lumotni (MMM) tizimga yuklaydi. Ma’lumot ixtiyoriy hajmda bo‘lishi mumkin. Amaliy jihatdan, katta hajmdagi fayllar bloklarga ajratiladi:

$M = \{M_1, M_2, \ldots, M_n\}$, $M = \{M_1, M_2, \ldots, M_n\}$, Bu yondashuv parallel shifrlash imkonini beradi va tizim samaradorligini oshiradi.Simmetrik shifrlash (AES - 256) har bir ma’lumot bloki tasodifiy generatsiya qilingan simmetrik kalit KsK_sKs yordamida shifrlanadi.Shifrlash jarayoni matematik jihatdan quyidagicha ifodalanadi:

$$C = \mathrm{AES}_{K_s}(M)$$

AES - funksiya nomi matn ko'rinishida

K_s - pastki indeks

(M) - funksiyaga uzatilgan xabar yoki bloklar bo‘yicha bu yerda:

$C_i = \mathrm{AES}_{K_s}(M_i), \quad i = 1, 2, \ldots, n$

MMM - ochiq matn, KsK_sKs - 256 - bitli simmetrik kalit, CCC - shifrlangan matn

AES algoritmining iterativ raund modeli:

$$S^{(i)} = \text{MixColumns}\Big(\text{ShiftRows}\Big(\text{SubBytes}(S^{(i-1)})\Big)\Big) \oplus K^{(i)}$$

$S^{(i)}$ i-bosqich holati

MixColumns, ShiftRows, SubBytes - funksiyalar , $\oplus$ - XOR amali

$K^{(i)}$ - i-bosqich kaliti

AES - 256 14 raunddan iborat bo‘lib, bu kriptobardoshlilikni sezilarli darajada oshiradi.Ilmiy asos simmetrik shifrlashning hisoblash murakkabligi taxminan:

$O(n)O(n)O(n)$ bo‘lib, bu katta hajmdagi ma’lumotlar bilan ishlashda yuqori samaradorlikni ta’minlaydi. Kalitni RSA yordamida shifrlash. Simmetrik kalitning xavfsiz uzatilishini ta’minlash maqsadida u RSA ochiq kaliti yordamida shifrlanadi.

RSA parametrlar generatsiyasi:

$n = p \times q$n]n n[$\varphi(n) = (p-1)(q-1)$n]n n [$e \cdot d \equiv 1 \pmod{\varphi(n)}$ kalitni shifrlash formulasi $E_k = K_s^e \bmod n$ bu yerda: eee - ochiq kalit eksponenti, nnn - modul, EkE_kEk - shifrlangan simmetrik kalit RSA hisoblash murakkabligi: $O(n^3)O(n^3)O(n^3)$ bo‘lib, u katta hajmli ma’lumot uchun emas, balki kichik hajmdagi kalitlarni shifrlash uchun samarali hisoblanadi. Shu sababli modelda faqat AES kaliti RSA yordamida shifrlanadi.Bulutga uzatish va saqlash. Bulut serverida quyidagi juftlik saqlanadi.

(C, E_k) bu yerda CCC - shifrlangan ma’lumot $E_k E_k E_k$ - shifrlangan simmetrik kalit

Shu bilan ma’lumotning o‘zi ham, kalit ham himoyalangan holatda saqlanadi.Simmetrik kalitni tiklash RSA yopiq kaliti yordamida $K_s = E_k^d \bmod n$ bu yerda ddd - yopiq kalit eksponenti. Tiklangan $K_s K_s K_s$ yordamida $M = \text{AES}_{K_s}^{-1}(C)$ Agar ma’lumot bloklarga bo‘lingan bo‘lsa: $M_i = \text{AES}_{K_s}^{-1}(C_i)$ natijada asl ma’lumot to‘liq tiklanadi.Metodologiyaning ilmiy afzalligi. Taklif etilgan model quyidagi ilmiy ustunliklarga ega.Tezkorlik va xavfsizlik o‘rtasida optimal muvozanat.Hisoblash yuklamasining kamayishi va kalit boshqaruvining markazlashmagan modeli [8].Bulutli arxitektura bilan moslashuvchan integratsiya.Modelning umumiy matematik ifodasi:

$$\begin{cases} C = \text{AES}_{K_s}(M) \\ E_k = K_s^e \bmod n \end{cases} \quad \text{Deshifrlash:} \quad \begin{cases} K_s = E_k^d \bmod n \\ M = \text{AES}_{K_s}^{-1}(C) \end{cases}$$

Taklif etilgan metod simmetrik va assimetrik kriptografiyaning hisoblash xususiyatlarini hisobga olgan holda ishlab chiqilgan. AES katta hajmdagi ma’lumotlarni tezkor shifrlashni ta’minlasa, RSA kalit almashinuvi xavfsizligini kafolatlaydi. Shu orqali bulutli hisoblash tizimlarida xavfsizlik va samaradorlik o‘rtasida barqaror muvozanat hosil qilinadi [7].

TAJRIBA NATIJALARI VA TAHLILI. Taklif etilgan gibrid kriptografik model samaradorligini baholash maqsadida eksperimental sinovlar o‘tkazildi [4]. Tajribalar turli hajmdagi (1 GB, 5 GB va 10 GB) ma’lumotlar ustida amalga oshirildi. Har bir algoritm uchun shifrlash jarayonining umumiy bajarilish vaqti (sekundlarda) o‘lchandi. Sinovlar quyidagi konfiguratsiyada amalga oshirildi:
Protsessor: 8 yadroli, 3.2 GHz**,** Operativ xotira: 16 GB RAM**,** Operatsion tizim: Linux 64 - bit**,** AES versiyasi: AES - 256**,** RSA versiyasi: RSA – 2048**,** Shifrlash rejimi: CBC Har bir tajriba 5 marta takrorlandi va o‘rtacha qiymatlar jadvalga kiritildi.

Natijalar jadvali

Hajm	AES (s)	RSA (s)	Gibrid (s)
1 GB	11	210	13
5 GB	54	1050	61
10 GB	108	2100	121

Hisoblash samaradorligi tahlilida AES algoritmida natijalar shuni ko‘rsatdiki, AES shifrlash vaqti ma’lumot hajmiga deyarli chiziqli bog‘liq: $T_{AES} \propto n$ Bu esa algoritmning vaqt murakkabligi: O(n)O(n)O(n) ekanligini tasdiqlaydi. 10 GB hajm uchun vaqt 108 soniyani tashkil etdi, bu katta hajmdagi ma’lumotlar uchun yuqori samaradorlikni ko‘rsatadi.RSA algoritmi esa katta hajmdagi ma’lumotlarda juda katta vaqt sarfladi. 10 GB fayl uchun 2100 soniya talab qilindi.Hisoblash murakkabligi taxminan: $O(n^3)O(n^3)O(n^3)$ bo‘lib, bu RSAning katta hajmli ma’lumotlar uchun mos emasligini ko‘rsatadi. RSA asosan kichik hajmli obyektlar (kalitlar) uchun samarali. Gibrid modelda. Ma’lumot AES yordamida shifrlanadi faqat 256 - bitli kalit RSA yordamida shifrlanadi. Shuning uchun umumiy vaqt

$T_{Hybrid} = T_{AES} + T_{RSA(\text{Key})}$ juda kichik qiymat bo‘lib, umumiy vaqtga sezilarli ta’sir qilmaydi. Natijalar shuni ko‘rsatadiki: 1 GB uchun AES - 11 s, Gibrid - 13 s, 10 GB uchun AES - 108 s, Gibrid - 121 s, Farq atigi 10 - 12% ni tashkil etadi. AES va Gibrid chiziqlari deyarli parallel.RSA chizig‘i keskin yuqoriga o‘suvchi. Bu shuni ko‘rsatadiki, gibrid model tezkorlik bo‘yicha AESga yaqin natija beradi ammo xavfsizlik jihatdan RSA darajasida himoya ta’minlaydi.Xavfsizlik darajasi tahlili. AES - 256 bruteforce hujumga nisbatan: 2^{256} murakkablikka ega. RSA - 2048 faktorizatsiya murakkabligi: $O\left(e^{(\log n)^{1/3}}\right)$ darajasida bo‘lib, amaliy jihatdan buzish deyarli imkonsiz hisoblanadi. Gibrid modelda ma’lumot AES bilan himoyalangan kalit RSA bilan himoyalangan.Shuning uchun tizimning umumiy xavfsizlik darajasi RSA bilan teng darajada yuqori deb baholanadi.Tajriba natijalari taklif etilgan gibrid kriptografik modelning samaradorligini tasdiqladi. Model hisoblash samaradorligi bo‘yicha AES darajasiga yaqin. Xavfsizlik darajasi bo‘yicha RSA bilan teng. Bulutli hisoblash muhitida amaliy qo‘llash uchun mos. Shunday qilib, xavfsizlik va tezkorlik o‘rtasida optimal muvozanatga erishildi [10].

MUHOKAMA. Eksperimental natijalar va nazariy tahlil asosida taklif etilgan gibrid kriptografik model bulutli hisoblash tizimlari uchun xavfsizlik va samaradorlik o‘rtasida optimal muvozanatni ta’minlashi aniqlandi. Ushbu bo‘limda modelning ustunliklari, amaliy qo‘llanish imkoniyatlari hamda istiqbolli rivojlanish yo‘nalishlari ilmiy nuqtai nazardan muhokama qilinadi [5].Modelning asosiy ustunliklari tezkorlik eksperimental natijalar shuni ko‘rsatdiki, gibrid modelning umumiy ishlash vaqti deyarli AES algoritmiga teng. Buning sababi - katta hajmdagi ma’lumotlar simmetrik algoritm yordamida shifrlanadi, RSA esa faqat kichik hajmdagi kalitni qayta ishlaydi. Nazariy jihatdan: $T_{\text{Hybrid}} = T_{\text{AES}} + T_{\text{RSA(Key)}}$ bu yerda $T_{\text{RSA}}(\text{Key})$ - juda kichik qiymat bo‘lib, umumiy hisoblash yuklamasiga sezilarli ta’sir ko‘rsatmaydi.Natijada model katta hajmli ma’lumotlar bilan ishlashda masshtablanuvchanlikni ta’minlaydi.Kalit almashinuvi xavfsizligi Simmetrik algoritmlarning asosiy muammosi - kalitni xavfsiz uzatish masalasidir. Gibrid modelda bu muammo RSA mexanizmi yordamida hal etiladi.RSA ochiq kalitli kriptotizim sifatida kalit almashinuvi jarayonida tomon ishtirokini xavfsiz tashkil etadi. Raqamli imzo va autentifikatsiya imkonini beradi.Ochiq tarmoq muhitida ma’lumot almashinuvi xavfsizligini ta’minlaydi.Shunday qilib, model ma’lumotlarning maxfiyligi

(confidentiality) va yaxlitligini (integrity) birgalikda himoyalaydi.Bulutli hisoblash arxitekturasi ko‘pincha quyidagi qatlamdan iborat.Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS). Ushbu model quyidagi platformalarda qo‘llanishi mumkin.SaaS darajasida - foydalanuvchi ma’lumotlarini shifrlash.PaaS darajasida - xavfsiz API va xizmatlar integratsiyasi.IaaS darajasida - virtual disklar va saqlash tizimlarini himoyalash.Gibrid modelning modulli tuzilishi uni turli xizmat arxitekturalariga integratsiya qilish imkonini beradi.Katta hajmdagi ma’lumotlarni (Big Data) qayta ishlashda hisoblash samaradorligi hal qiluvchi omil hisoblanadi. AES algoritmining chiziqli murakkabligi O(n)O(n)O(n) modelni katta hajmli fayllar bilan ishlash uchun mos qiladi. RSA esa faqat kalit darajasida ishlatilgani sababli tizim umumiy ishlash tezligiga salbiy ta’sir ko‘rsatmaydi.Model real vaqt rejimidagi bulutli servislar uchun ham qo‘llanishi mumkin.Taklif etilgan model ikki qatlamli himoya mexanizmini ta’minlaydi.Ma’lumotlar AES bilan shifrlanadi.Kalit RSA bilan himoyalanadi.Shu sababli hujumchi tizimni buzish uchun 256 - bitli AES kalitini bruteforce orqali aniqlashi yoki 2048 - bitli RSA modulini faktorizatsiya qilishi zarur bo‘ladi. AES bruteforce murakkabligi 2^{256} RSA faktorizatsiya murakkabligi esa sub ekspotensial darajada bo‘lib, amaliy jihatdan bajarib bo‘lmaydigan hisoblanadi.

Bu modelni kriptografik jihatdan barqaror deb baholash imkonini beradi.Amaliy qo‘llanilish imkoniyatlari taklif etilgan model quyidagi sohalarda qo‘llanishi mumkin.Bulutli ma’lumotlar omborlari,Elektron hukumat tizimlari,Moliyaviy va bank tizimlari,Tibbiy ma’lumotlar bazalari,Korporativ xavfsizlik tizimlari ayniqsa, maxfiylik talabi yuqori bo‘lgan tizimlarda model samarali natija beradi.Zamonaviy kriptografiya kvant hisoblash texnologiyalarining rivojlanishi bilan yangi bosqichga o‘tmoqda. Shuning uchun modelni quyidagi yo‘nalishlarda takomillashtirish istiqbolli hisoblanadi.Elliptic Curve Cryptography algoritmi RSAga nisbatan kichikroq kalit uzunligida yuqori xavfsizlikni ta’minlaydi. ECC asosidagi gibrid model hisoblash tezligini oshirishi kalit hajmini kamaytirishi, mobil va IoT muhitlari uchun moslashuvchanlikni ta’minlashi mumkin.Kvant kompyuterlari RSA kabi faktorizatsiyaga asoslangan algoritmlarni zaiflashtirishi mumkin. Shu sababli post - quantum cryptography (PQC) yo‘nalishi dolzarb hisoblanadi [7]. Lattice - based cryptography, hash - based signatures, code - based cryptosystems bilan integratsiya qilish xavfsizlikni yanada mustahkamlashi mumkin. Tadqiqot natijalari shuni ko‘rsatadiki, taklif etilgan gibrid kriptografik model bulutli hisoblash muhitida hisoblash samaradorligini saqlaydi,kalit boshqaruvi xavfsizligini ta’minlaydi,masshtablanuvchan arxitekturaga moslashadi,real tizimlarda amaliy qo‘llash imkonini beradi.Shunday qilib, model xavfsizlik va tezkorlik o‘rtasida muvozanatni ta’minlovchi optimal arxitektura sifatida baholanadi.

XULOSA. Mazkur tadqiqot natijalari shuni ko‘rsatdiki, AES - 256 va RSA - 2048 algoritmlariga asoslangan gibrid kriptografik model bulutli hisoblash tizimlarida ma’lumotlarni himoyalash uchun samarali va amaliy jihatdan asoslangan yechim hisoblanadi.Model simmetrik va assimetrik kriptografiyaning ustun jihatlarini birlashtirish orqali xavfsizlik va hisoblash samaradorligi o‘rtasida optimal muvozanatni ta’minlaydi.Eksperimental tahlillar shuni tasdiqladiki, katta hajmdagi ma’lumotlarni shifrlash jarayonida AES - 256 algoritmi yuqori tezkorlikni ta’minlaydi, RSA - 2048 esa kalit almashinuvi xavfsizligini kafolatlaydi.Gibrid modelda RSA faqat simmetrik kalitni shifrlash uchun qo‘llanilgani sababli umumiy hisoblash yuklamasi sezilarli darajada kamayadi. Natijada tizimning umumiy ishlash vaqti AES algoritmiga yaqin darajada saqlanib qoladi. Tadqiqot davomida quyidagi ilmiy natijalarga erishildi. Bulutli muhitda kriptografik himoya

arxitekturasi ishlab chiqildi. Simmetrik va assimetrik algoritmlarning kombinatsiyasi asosida samarali model taklif etildi.Modelning hisoblash samaradorligi va xavfsizlik darajasi eksperimental ravishda baholandi [7].Xavfsizlik va tezkorlik o‘rtasidagi muvozanat matematik va amaliy jihatdan asoslab berildi.Taklif etilgan model bulutli xizmatlarning turli qatlamlarida - SaaS, PaaS va IaaS arxitekturalarida - qo‘llanishi mumkin [10]. Ayniqsa, moliyaviy, tibbiy, davlat va korporativ axborot tizimlarida ma’lumotlar maxfiyligini ta’minlashda ushbu yondashuv samarali natija berishi kutiladi.Shuningdek, model modulli tuzilishga ega bo‘lgani sababli uni kelajakda elliptik egri chiziqli kriptografiya ECC yoki kvantbardosh algoritmlar bilan integratsiya qilish imkoniyati mavjud. Bu esa uzoq muddatli axborot xavfsizligini ta’minlashga xizmat qiladi.Umuman olganda, tadqiqot natijalari bulutli hisoblash tizimlarida ma’lumotlarni himoyalash masalasida gibrid kriptografik yondashuvning dolzarbligi va amaliy samaradorligini tasdiqlaydi.Taklif etilgan model xavfsizlik talablariga javob beruvchi, masshtablanuvchan va resurs tejamkor arxitektura sifatida baholanishi mumkin.

Adabiyotlar/Литература/References:

1. Stallings, W. Cryptography and Network Security: Principles and Practice. - 7th ed., Pearson, 2020.
2. 2.Paar, C., Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners. – Springer, 2019.
3. 3.National Institute of Standards and Technology (NIST). FIPS PUB 197: Advanced Encryption Standard (AES). - Gaithersburg, MD, 2001.
4. 4.Ron Rivest, Adi Shamir, Leonard Adleman. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Communications of the ACM, 21(2), 1978, pp. 120 - 126.
5. 5.IEEE. IEEE Transactions on Cloud Computing. – Vol. 11, No. 2, 2023.
6. 6.National Institute of Standards and Technology (NIST). SP 800-57 Part 1 Rev. 5: Recommendation for Key Management. – 2020.
7. 7.National Institute of Standards and Technology (NIST). SP 800-175B: Guideline for Using Cryptographic Standards in the Federal Government. – 2020.
8. 8.William Diffie, Martin Hellman. “New Directions in Cryptography.” IEEE Transactions on Information Theory, 22(6), 1976, pp. 644–654.
9. 9.Victor Miller. “Use of Elliptic Curves in Cryptography.” Advances in Cryptology - CRYPTO ’85, Springer, 1986.
10. 10.Aljawarneh, S., et al. “Hybrid Encryption Schemes for Secure Cloud Data Storage.” Journal of Cloud Computing, 2022, Vol. 11, Article 45.

ISSN: 3030-3702 (Online)
САЙТ: https://techscience.uz

TECHSCIENCE.UZ

TEXNIKA FANLARINING DOLZARB MASALALARI

№ 3 (4)-2026

TOPICAL ISSUES OF TECHNICAL SCIENCES

TECHSCIENCE.UZ- TEXNIKA FANLARINING DOLZARB MASALALARI elektron jurnali 15.09.2023-yilda 130346-sonli guvohnoma bilan davlat ro‘yxatidan o‘tkazilgan.
Muassislar: “SCIENCEPROBLEMS TEAM” mas’uliyati cheklangan jamiyati;
Jizzax politexnika insituti.

TAHRIRIYAT MANZILI:
Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog‘och ko‘chasi, 70/10-uy.
Elektron manzil:
scienceproblems.uz@gmail.com