MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI
JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

XALQARO ILMIY-TEXNIK ANJUMAN MATERIALLARI TO‘PLAMI

1-QISM

26-27-SENTABR
2025-YIL

doi Google Scholar

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MIRZO ULUG‘BEK NOMIDAGI O‘ZBEKISTON MILLIY UNIVERSITETINING JIZZAX FILIALI

KOMPYUTER ILMLARI VA MUHANDISLIK TEXNOLOGIYALARI

mavzusidagi Xalqaro ilmiy-texnik anjuman materiallari to‘plami

(2025-yil 26-27-sentabr)

1-QISM

JIZZAX-2025

Kompyuter ilmlari va muhandislik texnologiyalari. Xalqaro ilmiy-texnik anjuman materiallari to‘plami – Jizzax: O‘zMU Jizzax filiali, 2025-yil 26-27-sentabr. 355-bet.

Xalqaro miqyosidagi ilmiy-texnik anjuman materiallarida zamonaviy kompyuter ilmlari va muhandislik texnologiyalari sohasidagi innovatsion tadqiqotlar aks etgan.

Globallashuv sharoitida davlatimizni yanada barqaror va jadal sur’atlar bilan rivojlantirish bo‘yicha amalga oshirilayotgan islohotlar samarasini yaxshilash sohasidagi ilmiy-tadqiqot ishlariga alohida e’tibor qaratilgan. Zero iqtisodiyotning, ijtimoiy sohalarni qamrab olgan modernizatsiya jarayonlari, hayotning barcha sohalarini liberallashtirishni talab qilmoqda.

Ushbu ilmiy ma’ruza tezislari to‘plamida mamlakatimiz va xorijlik turli yo‘nalishlarda faoliyat olib borayotgan mutaxassislar, olimlar, professor-o‘qituvchilar, ilmiy tadqiqot institutlari va markazlarining ilmiy xodimlari, tadqiqotchilari, magistr va talabalarning ilmiy-tadqiqot ishlari natijalari mujassamlashgan.

Ma’ruf Ruzikulovich, Xafizadionov Usanitdin Nuratdin o‘g‘li. Axborot resurslaridan foydalanish ko‘rsatkichlarini normallashtirish asosida bilim oluvchilarning bilim darajasini baholash usullari Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali. Vol. 2, Issue 5, Toshkent, 2024. B. 91-96.

2. Kuvandikov J.T. Baholash ko‘rsatkichlarining ko‘p bosqichli tahlili asosida bilimlarni aks ettirishning noravshan mantiq asosida qaror qabul qilish algoritmi // Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali. – Vol. 2, Issue 5, Toshkent -2024. B. 83-90.

3. Kuvandikov J.T Intellektual o‘qitish tizimida bilim oluvchining noravshan modelini tashkil etish yondashuvi // Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali. – Vol. 2, Issue 1, Toshkent -2024. B. 49-55.

4. Raximov N.O., Kuvandikov J.T. Intellektual o‘qitish tizimlarini avtomatlashtirishda bilim oluvchi modelini loyihalashtirish // Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali. – Vol. 1, Issue 3,– Toshkent, 2023. B. 154-160.

5. Babomuradov O.J., Raximov N.O., Kuvandikov J.T. AKT sohasida kasbga yo‘naltirilgan o‘qitish samaradorligini oshirish // Innovatsion yondashuvlar ilm-fan taraqqiyoti kaliti sifatida: yechimlar va istiqbollar Respublika ilmiy-texnik anjuman Jizzax-2020 y. 266-272 –B.

6. Kuvandikov J.T., Daminova B.E., Xafizadinov U. N. Avtomatlashtirilgan elektron ta’lim tizimini loyihalashda o‘quv jarayonini modellashtirish // Qarshi davlat universiteti algoritmlar va dasturlashning dolzarb muammolari mavzusidagi xalqaro ilmiy-amaliy anjuman Qarshi-2023 y. 656-659 –B.

SHIFRLASH MEXANIZMLARINING DASTURIY TA’MINOT XAVFSIZLIGIGA TA’SIRINI INTELLEKTUAL TAHLIL QILISH

dots. Baratov Jasur Rustam o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali
Begmurodov Jaxongir Nizomiddin o‘g‘li, Abduvoitov Amirbek Nurboy o‘g‘li, Muxammadiyev G‘iyosiddin Jamshid o‘g‘li, Murodov Ne’mat Qaxramon o‘g‘li
O‘zbekiston Milliy universiteti Jizzax filiali talabalari
jasurjon2187@gmail.com

Annotatsiya: Maqolada dasturiy ta’minot xavfsizligida AES, RSA va ECC algoritmlarining matematik asoslari va amaliy samaradorligi tahlil qilindi. Intellektual tahlil yondashuvlari asosida ularning afzallik va cheklovlari ko‘rsatildi hamda kalit boshqaruvi jarayonlari milliy normativ talablar bilan uyg‘unlashtirildi.

Kalit so‘zlar: Dasturiy ta’minot xavfsizligi, shifrlash algoritmlari, AES, RSA, ECC, intellektual tahlil.

Axborot texnologiyalarining rivojlanishi dasturiy ta’minot xavfsizligini ta’minlashni dolzarb masalaga aylantirdi. Shifrlash mexanizmlari (AES, RSA, ECC va boshqalar) axborotni himoya qilishning asosiy vositasi bo‘lsa-da, zamonaviy kiberxavf-xatarlarning murakkablashuvi ularni intellektual tahlil qilish zaruratini yuzaga keltirmoqda[6]. Sun’iy intellekt va mashinaviy o‘rganishga asoslangan yondashuvlar shifrlash samaradorligini baholash, kalit boshqaruvini nazorat qilish hamda yangi xavfsizlik standartlariga mos innovatsion yechimlar ishlab chiqishda muhim rol o‘ynaydi.

Shifrlash mexanizmlarining dasturiy ta’minot xavfsizligiga ta’sirini tahlil qilishda bir nechta ilmiy-uslubiy yondashuvlar qo‘llanildi.

Birinchidan, mavjud kriptografik algoritmlar – AES, RSA, ECC kabi keng qo‘llaniladigan mexanizmlar ularning nazariy asoslari va amaliy samaradorligi nuqtayi nazaridan ko‘rib chiqildi [1, 2]. Ushbu algoritmlar xavfsizlik darajasi, hisoblash murakkabligi va resurs sarfi bo‘yicha solishtirildi.

Ikkinchidan, intellektual tahlil usullari – sun’iy intellekt va mashinaviy o‘rganish algoritmlari shifrlash jarayonlarini baholashga qo‘llandi. Xususan, shifrlash tezligi, kalit uzunligi, algoritmlarning tajovuzkor hujumlarga chidamliligi kabi parametrlar aniqlashda data mining va pattern recognition usullari asos sifatida tanlandi [3].

Uchinchidan, normativ-huquqiy asoslar tahlil qilindi. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonuni asosida shifrlash mexanizmlarini qo‘llashda amaliyotda talab etiladigan huquqiy normalar va standartlarga rioya etish jihatlari ko‘rib chiqildi [4].

To‘rtinchidan, amaliy tajriba sifatida turli shifrlash mexanizmlari dasturiy muhitda (C#, Python, Java) modellashtirildi va ularga intellektual tahlil vositalari qo‘llanilib, ularning samaradorligi bo‘yicha eksperimental natijalar yig‘ildi. Bu yondashuv orqali algoritmlarning dasturiy ta’minot xavfsizligiga real ta’siri baholandi.

Tadqiqot davomida dasturiy ta’minot xavfsizligini ta’minlashda keng qo‘llaniladigan uchta asosiy shifrlash mexanizmi – AES, RSA va ECC algoritmlari nazariy va amaliy jihatdan tahlil qilindi. Har bir algoritmning matematik asoslari, hisoblash murakkabligi va amaliy samaradorligi o‘rganildi.

AES algoritmi simmetrik blokli shifrlashga asoslanadi va 128 bitli bloklarda ishlaydi. Uning asosiy amallari Galois maydoni $GF(2^8)$ ustida bajariladi [1]. AES shifrlash jarayoni quyidagi tenglama orqali ifodalanadi:

$$C = E_K(P), \qquad P = D_K(C)$$

bu yerda P — ochiq matn, C — shifrlangan matn, K esa kalitni anglatadi. Har bir bosqichda SubBytes, ShiftRows, MixColumns va AddRoundKey amallari qo‘llanadi. Ayniqsa, AddRoundKey bosqichida blok va kalit o‘rtasida XOR amali bajariladi:

$$S_i = S_{i-1} \oplus K_i.$$

Olib borilgan hisoblashlar AES algoritmining tezligi yuqori ekanini va apparat tezlatkichlari mavjud bo‘lganda katta hajmdagi ma’lumotlarni real vaqt rejimida shifrlash imkonini berishini ko‘rsatdi.

RSA algoritmi esa assimetrik shifrlashga asoslangan bo‘lib, uning matematik poydevori katta asosiy sonlar va modul arifmetikasi bilan bog‘liq [2]. Kalit generatsiyasida $n = p \cdot q$ va $\varphi(n) = (p-1)(q-1)$ formulalari qo‘llanilib, $ed \equiv 1(mod\varphi(n))$ sharti bajarilishi zarur. Shifrlash va deshifrlash amallari quyidagicha ifodalanadi:

$$C \equiv P^e \ (mod\, n), \ P \equiv C^d (mod\, n).$$

RSA algoritmining afzalligi uning keng qo‘llanilishi va matematik asosining ishonchliligida bo‘lsa, kamchiligi – hisoblash tezligining pastligi va kalit uzunligining kattaligidadir. Masalan, 2048-bitli RSA amaliyotda xavfsizlik talablariga javob berishi mumkin, biroq uning ishlash tezligi AES yoki ECC ga qaraganda ancha past.

Elliptik egri chiziqlar asosidagi kriptografiya – ECC algoritmi, RSA ga nisbatan ancha qisqa kalitlar bilan yuqori darajadagi xavfsizlikni ta’minlaydi [3]. ECC quyidagi tenglama asosida ishlaydi:

$$E: y^2 = x^3 + ax + b \ (mod\, p),$$

bu yerda $a, b \in GF(p)$ va $4a^3 + 27b^2 \neq 0$. Algoritmda nuqtalar yig‘indisi va skalyar ko‘paytirish amallari qo‘llanadi, ya’ni $Q = kP$ ko‘rinishidagi amal shifrlash jarayonining markazida turadi. Kalit almashish jarayonida esa elliptik egri chiziqlarda Diffie–Hellman protokoli qo‘llanilib, $K = (k_A P_B) = (k_B P_A)$ shaklidagi umumiy kalit hosil qilinadi. Natijalar shuni ko‘rsatdiki, ECC-256 darajasi RSA-3072 bilan teng xavfsizlik darajasini beradi, ammo hisoblash xarajatlari 10–15 baravar kamroq.

Matematik va eksperimental tahlillar AES algoritmi katta hajmdagi ma’lumotlarni tezkor shifrlashda samarali ekanini, RSA esa ko‘proq raqamli imzo va kalit almashish uchun mos kelishini, ECC esa zamonaviy mobil va IoT tizimlarida xavfsizlik va samaradorlikning optimal muvozanatini ta’minlashini ko‘rsatdi.

Olib borilgan tadqiqot natijalari shuni ko‘rsatadiki, dasturiy ta’minot xavfsizligini ta’minlashda shifrlash mexanizmlarini tanlash nafaqat algoritmlarning nazariy barqarorligiga, balki ularning amaliy samaradorligiga ham bog‘liqdir. AES algoritmi blokli simmetrik shifrlash sifatida yuqori tezlik va real vaqt rejimida katta hajmdagi ma’lumotlarni qayta ishlash imkoniyatini ta’minlaydi. Ayniqsa, apparat darajasida qo‘llab-quvvatlanishi (AES-NI) uni zamonaviy tizimlarda standart yechim sifatida mustahkamlagan [8]. Biroq AESning asosiy cheklovlaridan biri kalit almashish mexanizmining tashqi protokollarga bog‘liq bo‘lishidir.

RSA algoritmi esa kuchli matematik asosga ega bo‘lsa-da, hisoblash murakkabligi va kalit uzunligining kattaligi sababli zamonaviy tizimlarda sekin ishlaydi[7]. Bu algoritm ko‘proq raqamli imzo va kalit almashish jarayonlarida qo‘llanilmoqda, biroq ma’lumotlar oqimlarini shifrlashda samaradorlik yetarli emas [2]. Shu bois RSAni keng ko‘lamli ma’lumotlarni qayta ishlashda emas, balki maxsus autentifikatsiya va ishonchni tasdiqlash bosqichlarida qo‘llash maqsadga muvofiqdir.

Elliptik egri chiziqlarga asoslangan ECC algoritmi esa qisqa kalitlar bilan yuqori darajadagi xavfsizlikni ta’minlashi bilan ajralib turadi. Tadqiqot natijalariga ko‘ra, ECC-256 bit darajasi RSA-3072 bit darajasiga teng xavfsizlik beradi, ammo hisoblash xarajatlari bir necha baravar kam. Shu sababli ECC algoritmi mobil qurilmalar va IoT tizimlarida optimal yechim sifatida tavsiya etiladi [3].

Muhim jihatlardan yana biri shifrlash mexanizmlarini qo‘llashda kalitlarni boshqarish va audit qilish jarayonidir. Kalitlarning yaratilishi, saqlanishi va rotatsiyasi, shuningdek, audit izlarini yuritish milliy va xalqaro standartlarga mos bo‘lishi shart. O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi Qonunida axborot resurslarini himoya qilish va kriptografik mexanizmlardan foydalanish bo‘yicha belgilangan talablar aynan shu jarayonlarda asosiy yo‘riqnoma bo‘lib xizmat qiladi [4, 8].

Umuman olganda, intellektual tahlil usullaridan foydalanish shifrlash algoritmlarini tanlash, kalitlarni boshqarish va xavfsizlik siyosatini optimallashtirishda sezilarli ustunlik beradi. Mashinaviy oʻrganish va maʼlumotlarni intellektual qayta ishlash texnologiyalari yordamida shifrlash mexanizmlarining notoʻgʻri qoʻllanilish hollari erta bosqichda aniqlanadi. Bu esa dasturiy taʼminot xavfsizligini oshirish, xavf-xatarlarni kamaytirish va kiberhujumlarga bardoshlilikni taʼminlashda muhim ilmiy-amaliy natija sifatida baholanadi.

Foydalanilgan adabiyotlar roʻyxati:

1. Stallings, W. *Cryptography and Network Security: Principles and Practice*. – 7th ed. – Boston: Pearson, 2021. – 912 p.
2. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. – 20th Anniversary Edition. – Hoboken: Wiley, 2019. – 784 p.
3. Boneh, D., Shoup, V. *A Graduate Course in Applied Cryptography*. – Stanford University, 2020. – 512 p. [Электронный ресурс]. – URL: https://toc.cryptobook.us/ (дата обращения: 20.09.2025).
4. Oʻzbekiston Respublikasi. "Kiberxavfsizlik toʻgʻrisida" Qonun. – Toshkent: Oʻzbekiston Respublikasi Qonun hujjatlari maʼlumotlari milliy bazasi, 2022. – №ЗРУ-781.
5. Mirzaev, N. M., Meliev, F. F., & Baratov, J. R. (2022). ARTIFICIAL INTELLIGENCE TECHNOLOGIES TO DETECT CANCERS FROM HUMAN COLON HISTOLOGICAL IMAGES. ББК 22.18 С 56, 181.
6. Baratov, J., & Xudoyqulov, D. (2024). DSA ALGORITMIDAN FOYDALANIB XAVFSIZ BO ʻLMAGAN TARMOQ ORQALI MAʼLUMOTLAR UZATISHNING AVTOMATLASHTIRILGAN TIZIMINI ISHLAB CHIQISH. *International Journal of scientific and Applied Research*, *1*(3), 126-132.
7. Жомуродов, Д. (2024). Интерактивное обучение кибербезопасности. *Новый Узбекистан: наука, образование и инновации*, *1*(1), 149-155.
8. Жомуродов, Д. (2024). Оптимизация и улучшение производительности алгоритма шифрования Blowfish. *Новый Узбекистан: наука, образование и инновации*, *1*(1), 155-158.

TALABALARNING YUTUQLARINI MONITORING QILISH VA BOSHQARISHNING ALGORITMIK YECHIMI: MENTORA DASTURIY TAʼMINOTI

Jomurodov Dustmurod Mamasoli oʻgʻli,
Meliyeva Mohira Zafar qizi
Oʻzbekiston Milliy universiteti Jizzax filiali

Annotatsiya. Mazkur maqolada talabalarning yutuqlarini monitoring qilish va boshqarishning algoritmik yondashuvlari, ularning Django framework asosida