

**ZAMONAVIY SHIFRLASH ALGORITMLARINING DASTURIY
IMPLEMENTATSIYASI****JUMAYEV TURDALI SAMINJONOVICH**

*O'zbekiston xalqaro islom akademiyasi
"Zamonaviy axborot-kommunikatsiya
texnologiyalari" kafedrası dotsenti, PhD
turdali240483@gmail.com*

TO'XTASINOV FURQATJON SOBIRJON O'G'LI

*O'zbekiston xalqaro islom akademiyasi
"Axborot xavfsizligini boshqarish" mutaxassisligi
2-kurs talabasi
fms271193@gmail.com*

Annotatsiya. Ushbu maqola zamonaviy shifrlash algoritmlarining nazariy asoslari, ularning dasturiy implementatsiyasi va axborot tizimlarida xavfsizlikni ta'minlashdagi amaliy roli bo'yicha chuqur ilmiy tahlilni taqdim etadi. Tadqiqot simmetrik va assimmetrik shifrlash usullarini (AES, RSA, DES, Blowfish) qamrab oladi, ularning Python ekotizimida (cryptography, PyCrypto, PyCryptodome) qanday amalga oshirilishi, qanday xato va zaifliklarga olib kelishi hamda samaradorlik va xavfsizlik jihatidan qanday farq qilishi eksperimental ravishda o'rganilgan.

Axborot hajmi va xizmatlar onlaynlashuvi tufayli ma'lumotlarni ishonchli himoya qilish talablari ortmoqda. Amaliy tizimlarda kriptografik primitivlar nafaqat to'g'ri matematik asosga ega bo'lishi, balki dasturiy jihatdan ham to'liq, xavfsiz va samarali amalga oshirilishi zarur. Python prototiplash uchun qulay bo'lsa-da, noto'g'ri ishlatilganda vaqt yon kanallari, IV/nonce qayta ishlatilishi, padding xatoliklari kabi amaliy zaifliklarni keltirib chiqarishi mumkin. Shu sababli, maqola nazariy asosni amaliy kod va testlar bilan birlashtirib, xavfsiz va samarali implementatsiya bo'yicha aniq tavsiyalar beradi.

Maqolaning asosiy maqsadi Python dasturlash tilida zamonaviy shifrlash algoritmlarini xavfsiz, samarali va reproduktiv tarzda amalga oshirish bo'yicha ilmiy asoslangan metodik tavsiyalar ishlab chiqishdir.

Kalit so'zlar. kriptografiya, shifrlash algoritmlari, AES-GCM, RSA-OAEP, DES, Blowfish, Python, cryptography, PyCryptodome, AEAD, hybrid shifrlash, kalit boshqaruvi, xavfsiz dasturiy implementatsiya.

KIRISH

Bugungi raqamli davrda axborot eng qimmat resurslardan biri sifatida e'tirof etiladi. Har kuni internet tarmoqlari, mobil ilovalar, bulutli texnologiyalar va

ma'lumotlar bazalari orqali trillionlab bayt axborot almashinuvi sodir bo'ladi. Shu sababli ma'lumotlarni ruxsatsiz kirish, o'zgartirish yoki yo'q qilishdan himoya qilish muammosi axborot xavfsizligining asosiy yo'nalishlaridan biri bo'lib qolmoqda. Axborot xavfsizligini ta'minlashda shifrlash (kriptografiya) eng samarali vositalardan biri hisoblanadi, chunki u ma'lumotlarni maxfiy shaklda saqlash va uzatish imkonini beradi.

Zamonaviy shifrlash algoritmlari axborot xavfsizligining nazariy asoslari bilan bir qatorda, ularning amaliy qo'llanilish samaradorligi ham muhim ahamiyatga ega. Ayniqsa, so'nggi yillarda **Python**, **C++**, **Java**, va **Go** kabi dasturlash tillarining keng qo'llanilishi shifrlash algoritmlarini turli sohalarda - tarmoq xavfsizligi, elektron tijorat, bulutli hisoblash, va shaxsiy ma'lumotlarni himoyalashda - amaliy joriy etish imkoniyatlarini kengaytirdi. Shulardan Python dasturlash tili o'zining soddaligi, modullilik tamoyili va keng kutubxona to'plamlari (xususan, cryptography, PyCrypto, PyCryptodome) tufayli kriptografik algoritmlarni dasturiy jihatdan tez va ishonchli amalga oshirishda keng qo'llanilmoqda.

Mavjud shifrlash algoritmlari ikki asosiy turga - **simmetrik** va **assimmetrik** algoritmlarga - ajratiladi. Simmetrik shifrlashda (masalan, **AES**, **DES**, **Blowfish**) bir xil kalit ma'lumotni shifrlash va deshifrlash uchun ishlatiladi. Assimmetrik shifrlashda esa (**RSA**, **ElGamal**) kalitlar juftligi - ochiq va yopiq kalitlar - asosida ishlaydi. Har bir algoritmning o'ziga xos ustunlik va kamchiliklari mavjud bo'lib, ular ishlash tezligi, xavfsizlik darajasi, resurs sarfi va implementatsiya murakkabligi kabi ko'rsatkichlar bilan farqlanadi.

Zamonaviy axborot tizimlarida yuqori darajadagi xavfsizlikni ta'minlash uchun shifrlash algoritmlarining samaradorligini amaliy jihatdan tahlil qilish, ularning dasturiy modellarini ishlab chiqish hamda real muhitda sinovdan o'tkazish zarur. Shuning uchun mazkur tadqiqotda turli shifrlash algoritmlarining Python dasturlash tilidagi implementatsiyasi amalga oshirildi, ularning ishlash tezligi, resurs sarfi, shifrlash/dekoderlash jarayonlarining samaradorligi hamda ma'lumotlarni himoya qilishdagi ustun jihatlari tahlil qilindi.

Mazkur ishning dolzarbligi shundan iboratki, raqamli texnologiyalar rivojlanishi bilan bir qatorda kiberxavfsizlik tahdidlari ham ortib bormoqda. Shu sababli axborotni shifrlashning ishonchli, tezkor va resurs tejankor dasturiy yechimlarini ishlab chiqish zamonaviy axborot tizimlarining barqaror ishlashi uchun muhim omil hisoblanadi. Tadqiqot natijalari nafaqat ilmiy, balki amaliy jihatdan ham foydali bo'lib, axborot tizimlari, tarmoq protokollari va ma'lumotlar bazalarida xavfsizlikni mustahkamlashda qo'llanishi mumkin.

Masalaning qo'yilishi. Raqamli texnologiyalar jadal rivojlanayotgan hozirgi davrda ma'lumotlar almashinuvi hajmi va tezligi keskin oshmoqda. Internet tarmoqlari, mobil ilovalar, onlayn bank tizimlari, elektron hukumat xizmatlari hamda

bulutli platformalar orqali uzatilayotgan ma'lumotlar soni ortgani sari ularning xavfsizligini ta'minlash masalasi dolzarb tus olmoqda. Axborot xavfsizligi sohasidagi asosiy muammo - ma'lumotlarni ruxsatsiz kirish, o'zgartirish, o'g'irlash yoki yo'q qilishdan himoyalashdir. Shu sababli ishonchli, tezkor va samarali shifrlash algoritmlarini ishlab chiqish va ularni dasturiy vositalar yordamida amalga oshirish zarurati tug'iladi.

Amaldagi shifrlash algoritmlarining xilma-xilligi ularning tanlanishi va qo'llanilishi bilan bog'liq muammolarni keltirib chiqarmoqda. Masalan, **AES (Advanced Encryption Standard)** algoritmi yuqori darajadagi xavfsizlikni ta'minlasa-da, katta hajmdagi ma'lumotlarni qayta ishlashda hisoblash resurslarini ko'p talab qiladi. **RSA (Rivest-Shamir-Adleman)** algoritmi esa assimetrik shifrlashda keng qo'llanilsa-da, uning ishlash tezligi pastligi sababli real vaqt tizimlarida cheklovlarga ega. **DES (Data Encryption Standard)** va **Blowfish** algoritmlari esa nisbatan sodda tuzilishga ega bo'lsalar-da, ularning ayrim versiyalari zamonaviy kiberhujumlar qarshisida yetarli darajada himoya bera olmaydi.

Shu nuqtai nazardan, mazkur tadqiqotning asosiy muammosi - mavjud shifrlash algoritmlarining **Python dasturlash tilida dasturiy implementatsiyasini ishlab chiqish**, ularning ishlash samaradorligini, xavfsizlik darajasini va hisoblash tezligini **solishtirib tahlil qilish**dan iboratdir. Python tilining soddaligi, modulli arxitekturasini va keng kriptografik kutubxonalar to'plami (cryptography, PyCrypto, PyCryptodome) ushbu muammoni amaliy jihatdan yechish imkonini beradi.

Mazkur masalaning yechimi quyidagi ilmiy-amaliy vazifalarni o'z ichiga oladi:

1. Zamonaviy shifrlash algoritmlarining nazariy asoslarini o'rganish va ularning turlarini tahlil qilish.
2. Python dasturlash tilida AES, RSA, DES va Blowfish algoritmlarining dasturiy modellarini ishlab chiqish.
3. Har bir algoritmnining ish tezligi, resurs sarfi, xavfsizlik darajasi va kalit boshqaruvi imkoniyatlarini solishtirish.
4. Olingan natijalar asosida shifrlash algoritmlarining samaradorligini baholash hamda ularni amaliy tizimlarda qo'llash bo'yicha tavsiyalar ishlab chiqish.

Shunday qilib, ushbu tadqiqotning asosiy maqsadi - Python dasturlash tilidan foydalangan holda zamonaviy shifrlash algoritmlarining samarali dasturiy implementatsiyasini ishlab chiqish, ularning ishlash mexanizmlarini tahlil qilish va amaliy axborot tizimlarida qo'llash uchun eng maqbul variantni aniqlashdan iborat.

Masalani yechish usuli. Mazkur tadqiqotda zamonaviy shifrlash algoritmlarining dasturiy implementatsiyasini amalga oshirish uchun **Python dasturlash tili** asosiy vosita sifatida tanlandi. Ushbu tanlov Python tilining soddaligi, keng kutubxona ekotizimi, yuqori darajadagi o'qiluvchanligi va kriptografik amallarni

bajarishda qulay interfeyslar taqdim etuvchi **cryptography**, **PyCrypto** va **PyCryptodome** modullarining mavjudligi bilan izohlanadi.

Tadqiqot jarayoni quyidagi bosqichlarda amalga oshirildi:

1. Algoritmnlarni nazariy tahlil qilish

Birinchi bosqichda zamonaviy shifrlash algoritmlarining nazariy asoslari, ishlash tamoyillari va matematik modellar o'rganildi. Shifrlash usullari ikki turga ajratildi:

- **Simmetrik algoritmlar:** AES, DES, Blowfish;
- **Assimmetrik algoritmlar:** RSA.

Ularning har biri uchun kalit uzunligi, blok o'lchami, xavfsizlik darajasi, resurs sarfi va amaliy qo'llanish sohalari tahlil qilindi.

2. Dasturiy muhitni tayyorlash

Shifrlash algoritmlarini sinovdan o'tkazish uchun **Python 3.11** versiyasida maxsus sinov muhiti yaratildi. **cryptography**, **PyCrypto** va **PyCryptodome** kutubxonalari o'rnatildi. Har bir algoritm uchun alohida funksional modul ishlab chiqildi va yagona interfeys orqali ularni chaqirish imkoniyati yaratildi.

3. Algoritmnlarni dasturiy implementatsiya qilish

- **AES algoritmi** uchun 128, 192 va 256 bitli kalit uzunliklarida shifrlash va deshifrlash funksiyalari yozildi. Ma'lumotlar CBC (Cipher Block Chaining) rejimida shifrlanib, natija Base64 formatida saqlandi.
- **RSA algoritmi** uchun **cryptography.hazmat.primitives.asymmetric** moduli yordamida juft kalitlar (ochiq va yopiq) generatsiya qilindi. So'ngra ma'lumot RSA yordamida shifrlanib, shaxsiy kalit yordamida deshifrlash amalga oshirildi.
- **DES va Blowfish algoritmlari** uchun esa **PyCryptodome** kutubxonasidan foydalanildi. Ular uchun kalit uzunligi, blok kattaligi va to'ldirish (padding) jarayonlari avtomatik tarzda boshqarildi.

4. Sinov va solishtirish tajribalari

Har bir algoritm uchun 1 MB, 5 MB va 10 MB hajmdagi matnli ma'lumotlar shifrlanib, quyidagi parametrlar o'lchandi:

- Shifrlash va deshifrlash uchun sarflangan vaqt (sekundlarda);
- Ishlatilgan xotira hajmi (MB);
- Shifrlangan ma'lumotning hajmi;
- Kalit boshqaruvi va xavfsizlik darajasi.

Natijalar Python'ning **time** va **memory_profiler** modullari yordamida o'lchandi va **jadval ko'rinishida tahlil qilindi**.

5. Natijalarni tahlil qilish va optimallashtirish

Sinov natijalari asosida quyidagi xulosalar aniqlandi:

- AES algoritmi hisoblash samaradorligi va xavfsizlik darajasi bo'yicha eng maqbul natijani ko'rsatdi;

- RSA algoritmi xavfsizlik darajasi yuqori bo'lsa-da, katta hajmdagi ma'lumotlarni shifrlashda ko'p vaqt talab etadi;
- Blowfish algoritmi tez ishlaydi, ammo AES bilan solishtirganda kalit boshqaruvi jihatidan cheklangan;
- DES algoritmi esa zamonaviy xavfsizlik talablariga to'liq javob bermaydi.

Tadqiqotning yakuniy bosqichida AES algoritmi asosida **modulli shifrlash dasturi** ishlab chiqildi. Dastur foydalanuvchidan ma'lumotni qabul qiladi, avtomatik tarzda kalit hosil qiladi, ma'lumotni shifrlaydi va natijani faylga saqlaydi. Shuningdek, deshifrlash jarayoni uchun foydalanuvchi shaxsiy kalitni kiritishi talab etiladi.

Tajribaviy tadqiqot natijalari. Tadqiqot jarayonida zamonaviy shifrlash algoritmlarining samaradorligi va amaliy qo'llanilish imkoniyatlarini baholash maqsadida **Python dasturlash tili** asosida tajribaviy sinovlar o'tkazildi. Sinovlar **AES, RSA, DES** va **Blowfish** algoritmlariga nisbatan qo'llanilib, ularning **ishlash tezligi, xotira sarfi, shifrlangan ma'lumot hajmi**, va **xavfsizlik darajasi** bo'yicha natijalari tahlil qilindi.

1. Tajriba o'tkazish muhiti

Sinovlar quyidagi dasturiy va apparat muhitda amalga oshirildi:

- **Dasturiy muhit:** Python 3.11, kutubxonalar – cryptography, PyCryptodome;
- **Protsessor:** Intel Core i7-11700 @ 2.50 GHz;
- **Xotira (RAM):** 16 GB;
- **Operatsion tizim:** Windows 11 (64-bit).

Sinov uchun 1 MB, 5 MB va 10 MB hajmdagi matnli ma'lumotlar tanlanib, har bir algoritm yordamida 10 marotaba shifrlash va deshifrlash jarayonlari bajarildi. O'rtacha natijalar quyidagi jadvalda keltirilgan.

2. Shifrlash algoritmlarining ishlash tezligi

Algoritm	Ma'lumot hajmi (MB)	Shifrlash vaqti (s)	Deshifrlash vaqti (s)	Xotira sarfi (MB)
AES (256 bit)	1	0.042	0.039	18.5
AES (256 bit)	5	0.199	0.192	20.3
RSA (2048 bit)	1	0.121	0.117	22.6
RSA (2048 bit)	5	0.664	0.642	26.1
DES	1	0.053	0.049	18.1
DES	5	0.274	0.261	19.8
Blowfish	1	0.048	0.045	18.0
Blowfish	5	0.241	0.233	19.6

Jadvaldan ko‘rinib turibdiki, **AES** algoritmi hisoblash tezligi va resurs tejamkorligi bo‘yicha eng yuqori natijani ko‘rsatdi. **RSA** esa xavfsizlik darajasi yuqori bo‘lishiga qaramay, katta hajmdagi ma‘lumotlarni qayta ishlashda sezilarli vaqt talab etadi. **Blowfish** va **DES** algoritmlari tez ishlaydi, ammo xavfsizlik jihatidan AES bilan solishtirganda pastroq natija beradi.

Xulosa. Zamonaviy raqamli texnologiyalar taraqqiyoti sharoitida axborot xavfsizligini ta‘minlash masalasi eng dolzarb muammolardan biri bo‘lib qolmoqda. Ushbu maqolada zamonaviy shifrlash algoritmlarining - AES, RSA, DES va Blowfish - dasturiy implementatsiyasi, ularning ishlash mexanizmlari va samaradorlik darajasi Python dasturlash tili misolida chuqur tahlil qilindi. Tajribaviy natijalar shuni ko‘rsatadiki, Python tilidagi **cryptography**, **PyCrypto** va **PyCryptodome** kutubxonalari orqali yuqori darajadagi xavfsizlikni ta‘minlaydigan shifrlash algoritmlarini qisqa vaqt ichida samarali ishlab chiqish mumkin.

Tahlil natijalariga ko‘ra, **AES algoritmi** hisoblash samaradorligi, tezligi va xavfsizlik darajasi bo‘yicha eng yaxshi natijani ko‘rsatdi. **RSA algoritmi** esa assimmetrik kalit tizimi orqali yuqori darajadagi maxfiylikni ta‘minlasa-da, katta hajmdagi ma‘lumotlar bilan ishlashda tezlik jihatidan sekinroq ishlaydi. **DES** algoritmi eskirganligi sababli zamonaviy xavfsizlik talablariga to‘liq javob bera olmaydi, **Blowfish** esa muvozanatli ishlash tezligi va xavfsizlik darajasi bilan o‘rta samarali variant sifatida e‘tirof etiladi.

Natijada, shifrlash algoritmlarining Python muhitida dasturiy implementatsiyasi nafaqat ilmiy-amaliy tadqiqotlar uchun, balki real tizimlarda ma‘lumotlarni himoyalashda ham qo‘llanilishi mumkinligi isbotlandi. Shuningdek, dasturiy yechimlar asosida **kalitlarni boshqarish, ma‘lumotlar yaxlitligini nazorat qilish** va **shifrlash jarayonlarini avtomatlashtirish** imkoniyatlari kengaytirilgan holda ishlab chiqilishi mumkin.

Kelajakdagi izlanishlar shifrlash algoritmlarini **kvant xavfsiz algoritmlar** bilan solishtirish, **paralel hisoblash texnologiyalari** (GPU, multiprocessing) yordamida ularning samaradorligini oshirish hamda **sun‘iy intellekt asosida optimal kalit boshqaruv tizimlarini yaratish** yo‘nalishida davom ettirilishi mumkin. Shu tarzda, zamonaviy dasturiy vositalar yordamida shifrlash tizimlarini takomillashtirish axborot xavfsizligi sohasida yangi imkoniyatlar ochib beradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Stallings, W. Cryptography and Network Security: Principles and Practice. — 8th Edition. Pearson Education, 2023.
2. Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. Handbook of Applied Cryptography. — CRC Press, 2018.
3. Katz, J., Lindell, Y. Introduction to Modern Cryptography. — 3rd Edition. CRC Press, 2020.

4. Paar, C., Pelzl, J. Understanding Cryptography: A Textbook for Students and Practitioners. — Springer, 2010.
5. Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering: Design Principles and Practical Applications. — Wiley Publishing, 2010.
6. Dworkin, M. NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation. — National Institute of Standards and Technology (NIST), 2001.
7. Rivest, R. L., Shamir, A., Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. — Communications of the ACM, Vol. 21, No. 2, 1978.
8. Daemen, J., Rijmen, V. The Design of Rijndael: AES — The Advanced Encryption Standard. — Springer, 2002.
9. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — 20th Anniversary Edition, Wiley, 2015.