FAYLLARNI SHIFRLASH VA DESHIFRLASHDA CRYPTOGRAPHY KUTUBXONASINING ILMIY ASOSLARI

Tojimamatov Israil Nurmamatovich
Farg‘ona davlat unversiteti katta o‘qituvchisi
israiltojimamatov@gmail.com
Lazokatoy Rahimova
Farg‘ona shahar 32-umumta’lim maktabi o‘qituvchisi
Tursunova Azimaxon Alijon qizi
Farg‘ona davlat unversiteti 3-kurs talabasi
azimaxontursunova676@gmail.com

Annotatsiya: Ushbu maqolada zamonaviy kriptografiya vositalaridan biri — Python dasturlash tilida keng qo‘llanilayotgan cryptography kutubxonasining ilmiy-texnik imkoniyatlari asosida fayllarni shifrlash va deshifrlash jarayonlari tahlil qilinadi. Maqolada simmetrik shifrlashning nazariy asoslari, xususan, Fernet algoritmi asosida xavfsiz va ishonchli ma’lumot almashinuvi tashkil etish yo‘llari ko‘rib chiqiladi. Kalitlar generatsiyasi, ularning saqlanish mexanizmlari, vaqt tamg‘asi (timestamp), autentifikatsiya va ma’lumot yaxlitligini ta’minlash kabi masalalar bo‘yicha chuqur ilmiy izohlar berilgan. Shuningdek, maqolada real dasturiy kodlar asosida faylni shifrlash va uni muvaffaqiyatli deshifrlash bosqichlari tahlil qilinadi. Kriptografik vositalarning amaliy jihatlari, foydalanuvchilarga havfsizlikni mustahkamlashda qanday imkoniyatlar berishi, shuningdek xatoliklarning oldini olishda qanday texnik chora-tadbirlar ko‘rilishi kerakligi yuzasidan fikr yuritiladi. Mazkur maqola nafaqat dasturchilar, balki axborot xavfsizligi bilan shug‘ullanuvchi mutaxassislar uchun ham nazariy va amaliy qo‘llanma bo‘lib xizmat qiladi.

Kalit so‘zlar: kriptografiya, shifrlash, deshifrlash, cryptography, Python, Fernet, AES, kalit generatsiyasi, xavfsizlik.

Abstract: This scientific article investigates the processes of file encryption and decryption using the cryptography library in Python, one of the most prominent tools in modern cryptography. The paper focuses on the implementation of symmetric encryption based on the Fernet algorithm, which combines AES encryption with HMAC authentication and timestamp verification to ensure both confidentiality and integrity. It explores key generation techniques, secure storage of keys, and the importance of handling decryption errors, unauthorized access, and data tampering. Practical code examples illustrate the step-by-step processes of encrypting and decrypting files securely. Moreover, the paper emphasizes the practical value of cryptographic tools in building secure communication systems and outlines the technical measures necessary to prevent common cryptographic failures. This study

serves as a theoretical and practical guide not only for Python developers but also for professionals in information security.

Keywords: cryptography, encryption, decryption, cryptography library, Python, Fernet, AES, key generation, security.

Аннотация: В данной статье исследуются процессы шифрования и дешифрования файлов с использованием библиотеки cryptography на языке Python, которая является одним из ключевых инструментов в современной криптографии. Основное внимание уделено симметричному шифрованию с применением алгоритма Fernet, сочетающего шифрование AES, аутентификацию HMAC и проверку временной метки для обеспечения конфиденциальности и целостности данных. В статье рассматриваются методы генерации ключей, их безопасное хранение, а также важность обработки ошибок при дешифровке, предотвращения несанкционированного доступа и подделки данных. Практические примеры кода иллюстрируют этапы надёжного шифрования и восстановления файлов. Кроме того, подчеркивается роль криптографических средств в построении защищенных информационных систем и приводятся технические рекомендации по предотвращению типичных ошибок. Работа может служить теоретическим и практическим пособием как для разработчиков, так и для специалистов по информационной безопасности.

Ключевые слова: криптография, шифрование, дешифрование, библиотека cryptography, Python, Fernet, AES, генерация ключей, безопасность.

Axborot texnologiyalari jadal rivojlanayotgan hozirgi davrda ma’lumotlar xavfsizligini ta’minlash — zamonaviy informatsion tizimlar arxitekturasi uchun asosiy talablar sirasiga kiradi. Har qanday axborot resursi, ayniqsa, shaxsiy, moliyaviy yoki ilmiy ma’lumotlar uchinchi tomon tomonidan ruxsatsiz qo‘lga kiritilish xavfi ostida bo‘ladi. Ushbu xavfning oldini olishning eng samarali usullaridan biri bu kriptografik shifrlash tizimlaridan foydalanishdir.

Akademik manbalarda qayd etilishicha, kriptografiya — bu ma’lumotni yashirish, uzatishda uni o‘zgartirish, shuningdek, ma’lumotlar yaxlitligini va autentifikatsiyasini ta’minlovchi fan sohasidir (Menezes, van Oorschot & Vanstone, *Handbook of Applied Cryptography*, 1996). Kompyuter fanlari va axborot xavfsizligi sohasida, ayniqsa, dasturiy ta'minot orqali amalga oshiriladigan shifrlash algoritmlari keng qo‘llaniladi. Ulardan biri bu — Python tilidagi cryptography kutubxonasi bo‘lib, foydalanuvchilarga kuchli va zamonaviy shifrlash imkoniyatlarini taqdim etadi.

Kriptografiya so‘zi yunoncha “kriptos” – yashirin va “grapho” – yozmoq so‘zlaridan kelib chiqqan bo‘lib, ma’lumotni boshqa shaxslar tushunmaydigan shaklda uzatish usullarini o‘rganadi. Dastlab kriptografiya harbiy va diplomatik maqsadlarda

qo‘llanilgan bo‘lsa-da, hozirda u internet orqali yuborilayotgan har qanday axborot uchun zaruriy himoya vositasiga aylangan.

Simmetrik va assimetrik kriptografiya mavjud:

1) Simmetrik kriptografiyada bitta umumiy kalit yordamida ma’lumot shifrlanadi va o‘sha kalit bilan deshifrlanadi (masalan: AES, Fernet).
2) Assimetrik kriptografiyada ikkita kalit ishlatiladi: ochiq (public) va yopiq (private) (masalan: RSA, ECC).

Simmetrik algoritmlar tezkorligi bilan ajralib turadi, fayl shifrlash va deshifrlashda aynan simmetrik algoritmlar — ayniqsa AES (Advanced Encryption Standard) asosida ishlovchi cryptography.fernet moduli qo‘llaniladi (Stallings, *Cryptography and Network Security*, 2017).

cryptography Python kutubxonasi (hazmat va fernet modullari asosida) kriptografik vositalarning sodda API sini taqdim etadi. U AES-128 algoritmiga asoslangan Fernet modulini o‘z ichiga oladi. Fernet — shifrlashning xavfsiz, protokolga asoslangan shakli bo‘lib, quyidagilarni o‘z ichiga oladi:

1) AES algoritmi
2) HMAC bilan autentifikatsiya
3) Timestamp asosida amal qilish muddati

Kalit generatsiyasi:

```
from cryptography.fernet import Fernet
key = Fernet.generate_key()
```

Shifrlash:

```
f = Fernet(key)
encrypted = f.encrypt(b"maxfiy matn")
```

Deshifrlash:

```
decrypted = f.decrypt(encrypted)
```

cryptography kutubxonasi yordamida fayllarni ham shifrlash va deshifrlash mumkin, bu amaliyot real tizimlarda (masalan, fayl zaxiralash, arxivlash, serverdan yuborishda) keng qo‘llaniladi.

Python tilidagi fayl shifrlash amaliyoti quyidagi bosqichlarda amalga oshiriladi:

Bosqich	Tavsifi
1. Kalit yaratish	Fernet.generate_key() orqali
2. Kalitni saqlash	.key fayliga yoziladi
3. Faylni o‘qish	open(filename, 'rb')
4. Shifrlash	f.encrypt(data)
5. Yangi faylga yozish	open(filename + '.enc', 'wb')

Bosqich	Tavsifi
6. Deshifrlash	f.decrypt(data) va saqlash

Bu jarayonlar kriptografik xavfsizlikning asosiy tamoyillariga (mahfiylik, yaxlitlik, mavjudlik) amal qilgan holda tashkil etiladi (Pfleeger & Pfleeger, *Security in Computing*, 2015).

Shifrlash algoritmi qanday mukammal bo‘lmasin, insonga bog‘liq xatoliklar (masalan, kalitni noto‘g‘ri saqlash, noto‘g‘ri deshifrlash urinishlari) xavfsizlikka putur yetkazadi. Shu sababli quyidagi tavsiyalar beriladi:

1) Shifrlash kalitlari faqat maxfiy joyda saqlansin (masalan: .env fayl, maxfiy server).
2) Har bir sessiyada yangicha kalit generatsiya qilinishi tavsiya etiladi.
3) Fayl uzatishdan oldin HMAC yordamida yaxlitlik tekshirilsin.
4) Fayl deshifrlashdan oldin timestamp tekshirish orqali yaroqlilik nazorat qilinsin.

Xulosa: Zamonaviy raqamli davrda axborot xavfsizligini ta’minlash har qanday texnologik jarayonning ajralmas qismidir. Ma’lumotlar xavfsizligi va maxfiyligi bilan bog‘liq masalalar har doim dolzarb bo‘lib kelgan va hozirgi kunda yanada muhimlashgan. Shuning uchun, shifrlash texnologiyalarining samaradorligi va ishonchliligi har bir tizimning muvaffaqiyatiga bevosita ta’sir ko‘rsatadi. Python dasturlash tilidagi cryptography kutubxonasi orqali yuqori darajadagi xavfsiz, ishonchli va amaliy shifrlash tizimini yaratish mumkin. Ushbu kutubxona nafaqat shifrlash va deshifrlash operatsiyalarini amalga oshirish imkonini beradi, balki foydalanuvchilarga xavfsiz kalit generatsiyasi, autentifikatsiya, va ma’lumot yaxlitligini ta’minlash kabi yuqori xavfsizlik darajasini kafolatlaydigan xususiyatlarni ham taklif etadi.

Bu esa nafaqat dasturchilar, balki ilmiy, tibbiy, moliyaviy va boshqa ko‘plab sohalar vakillari uchun ham muhim vositadir. Masalan, tibbiy ma’lumotlar yoki moliyaviy hisobotlar kabi maxfiy ma’lumotlarni himoya qilishda shifrlash texnologiyalarining ahamiyati kattadir. Ushbu tizimlar nafaqat ichki xavfsizlikni ta’minlashda, balki tashqi tahdidlarga qarshi kurashishda ham muhim rol o‘ynaydi. Xususan, Fernet algoritmi orqali amalga oshirilgan simmetrik shifrlash va uning imkoniyatlari har xil sohalarda ishonchli va tezkor yechimlar taqdim etadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Menezes A., van Oorschot P., Vanstone S. (1996). *Handbook of Applied Cryptography*. CRC Press.
2. Stallings W. (2017). *Cryptography and Network Security: Principles and Practice*. Pearson Education.
3. Pfleeger C.P., Pfleeger S.L. (2015). *Security in Computing*. Prentice Hall.

4. Ferguson N., Schneier B., Kohno T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Paar C., Pelzl J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
6. Official Python cryptography library documentation: https://cryptography.io
7. Tojimamatov, I., Soliyeva, X., & Israilova, R. (2025). FAYL NOMLARINI QISQARTIRISH ALGORITMLARI. Академические исследования в современной науке, 4(26), 45-52.
8. Nurmamatovich, T. I. (2025). MONGODB DA BIG DATA BILAN ISHLASH USULLARI. YANGI O‘ZBEKISTON, YANGI TADQIQOTLAR JURNALI, 2(8), 792-798.
9. Nurmamatovich, T. I. (2025). MOBIL OPERATSION SISTEMALARNING KELAJAGI. Лучшие интеллектуальные исследования, 44(5), 133-139.
10. Nurmamatovich, T. I., & Umidjon o‘g, M. Z. S. (2025). BERILGANLAR BAZASIDA HAYOTIY SIKL. Лучшие интеллектуальные исследования, 44(5), 169-178.
11. Nurmamatovich, T. I., & Umidjon o‘g, M. Z. S. (2025). MASHINA KODLARI BILAN ISHLASH. Лучшие интеллектуальные исследования, 44(5), 159-168.
12. Nurmamatovich, T. I. (2025). BERILGANLAR BAZASI ADMINISTRATORI. Лучшие интеллектуальные исследования, 44(5), 276-282.
13. Tojimamatov, I. (2025). ADO-NET TEXNOLOGIYASI YORDAMIDA HISOBOTLAR VA FORMALARNI SHAKLLANTIRISH. Академические исследования в современной науке, 4(25), 122-126.
14. Nurmamatovich, T. I. (2025). STATISTIKA SOHASIDA AXBOROT TIZIMLARI VA TEXNOLOGIYALARINI SINTAKSIS TAXLIL QILISH. Лучшие интеллектуальные исследования, 44(4), 157-166.
15. Nurmamatovich, T. I. (2025). AXBOROTLARNI TAQDIM ETISH VA ULAR BILAN ISHLASH. Лучшие интеллектуальные исследования, 44(4), 135-140.
16. Tojimamatov, I., & Abduvaliyev, X. (2025). KO ‘P FOYDALANUVCHILI BBBT ARXITEKTURASI. Инновационные исследования в науке, 4(5), 16-22.
17. Tojimamatov, I., & Xolmurod o‘g, A. O. H. (2025, May). SQL SERVERDA CHEKLASHLAR. In CONFERENCE OF MODERN SCIENCE & PEDAGOGY (Vol. 1, No. 1, pp. 409-413).
18. Tojimamatov, I., & Abdulhafizov, I. (2025). OBYEKTLAR VA ATRIBUTLAR. BRIDGING THE GAP: EDUCATION AND SCIENCE FOR A SUSTAINABLE FUTURE, 1(1), 107-112.
19. Tojimamatov, I. N., & Iminova, G. I. (2025). SEMANTIK OBEKT MODELI VA KATTA MA'LUMOTLAR (BIG DATA). ОБРАЗОВАНИЕ И НАУКА В XXI ВЕКЕ, (58-3).