Axborotlarni himoyalashda python daturlash tilining imkoniyatlari

Axatov Abror Asqar o‘g‘li
Sharof Rashidov nomidagi Samarqand davlat universiteti
abroraxatov10@gmail.com

Annotatsiya. *Ushbu maqolada axborot xavfsizligini ta’minlashda Python dasturlash tilining imkoniyatlari va vositalari o'rganiladi. Pythonning kriptografiya sohasidagi qo‘llanilishining afzalliklari, shuningdek, shifrlash, xeshlash, raqamli imzo yaratish va xavfsiz aloqa protokollarini qo‘llash kabi amaliyotlar tahlil qilinadi. Python o‘zining qulay sintaksisi, keng kutubxonalari va yuqori samaradorligi bilan kiberxavfsizlik va kriptografik vazifalarni bajarishda keng qo‘llaniladi va ushbu maqola axborotlarni himoya qilishda Python kutubxonalaridan, xususan, Cryptography, PyCryptodome va hashlib kabi modullardan foydalanish imkoniyatlarini tahlil qiladi. Ma’lumotlarni shifrlash va himoyalash bo‘yicha zamonaviy yechimlar va muammolarga Pythonning innovatsion yondashuvlari tavsiflanadi.*

Kalit so'zlar: *Python dasturlash tili, axborot xavfsizligi, kriptografiya, ma'lumotlarni shifrlash, simmetrik shifrlash, asimmetrik shifrlash, RSA algoritmi, AES algoritmi, CBC, raqamli imzo, ma'lumotlarni maxfiyligi, shaxsiy kalitlar, verifikasiya, kiberxavfsizlik, xesh funksiyalar.*

Аннотация. *В данной статье исследуются возможности и инструменты языка программирования Python для обеспечения безопасности информации. Анализируются преимущества использования Python в области криптографии, а также практики, такие как шифрование, хеширование, создание цифровых подписей и применение безопасных коммуникационных протоколов. Python широко применяется в кибербезопасности и криптографических задачах*

благодаря своей удобной синтаксической конструкции, обширным библиотекам и высокой эффективности. В статье рассматриваются возможности использования библиотек Python, таких как Cryptography, PyCryptodome и hashlib, для защиты информации. Описываются современные решения и проблемы шифрования и защиты данных, а также инновационные подходы Python.

Ключевые слова: *язык программирования Python, безопасность информации, криптография, шифрование данных, симметричное шифрование, ассиметричное шифрование, алгоритм RSA, алгоритм AES, CBC, цифровая подпись, конфиденциальность данных, личные ключи, верификация, кибербезопасность, хеш-функции.*

Annotation: *This article explores the capabilities and tools of the Python programming language for ensuring information security. It analyzes the advantages of using Python in the field of cryptography, as well as practices such as encryption, hashing, digital signature creation, and the application of secure communication protocols. Python is widely used in cybersecurity and cryptographic tasks due to its user-friendly syntax, extensive libraries, and high efficiency. This article examines the possibilities of using Python libraries, particularly modules such as Cryptography, PyCryptodome, and hashlib, for protecting information. Modern solutions and challenges in data encryption and protection are described, along with Python's innovative approaches.*

Keywords: *Python programming language, information security, cryptography, data encryption, symmetric encryption, asymmetric encryption, RSA algorithm, AES algorithm, CBC, digital signature, data confidentiality, private keys, verification, cybersecurity, hash functions.*

Raqamli asrning shiddat bilan rivojlanishi axborotlarni xavfsiz saqlash va himoyalash masalasini dolzarb muammolardan biriga aylantirdi. Har kuni milliardlab ma'lumotlar almashinuvi amalga oshiriladi, va ushbu jarayonda ma'lumotlarni to‘g‘ri boshqarish hamda ularni begona ko‘zlardan himoyalash katta ahamiyat kasb etadi. Shaxsiy ma'lumotlar, moliyaviy tranzaktsiyalar, intellektual mulk va boshqa turdagi maxfiy axborotlar ko‘pincha kiberhujumlar va tahdidlarga duch keladi. Kiberhujumlarning doimiy o‘sishi, tashkilot va shaxsiy foydalanuvchilarni himoya choralarini kuchaytirishga majbur qilmoqda[1-3].

Axborot xavfsizligi sohasida asosiy e’tibor ma’lumotlarni shifrlash, yaxlitligini saqlash va kirishni cheklashga qaratilgan. **Kriptografiya** – bu sohada eng muhim vositalardan biri hisoblanadi, chunki u ma’lumotlarni kodlash orqali ularning maxfiyligini ta'minlaydi. Zamonaviy texnologiyalarda kriptografik vositalardan foydalanish ko‘plab tizimlarda asosiy xavfsizlik chorasiga aylangan.

Python dasturlash tili ushbu jarayonlarda sezilarli o‘rin egallaydi. Uning soddaligi va qulay sintaksisi, shu bilan birga, kuchli kutubxonalari, pythonni axborot xavfsizligi va kriptografiya sohasida samarali vositaga aylantirdi. Ayniqsa, shifrlash algoritmlari bilan ishlash, ma’lumotlarni xeshlash, raqamli imzolar yaratish va tekshirish, xavfsiz aloqa protokollarini qo‘llash kabi vazifalarda python yetakchi dasturlash tillaridan biri hisoblanadi[4-8].

Ushbu maqola python dasturlash tilining axborotlarni himoyalash va kriptografiyada qo‘llanishiga bag‘ishlangan. Python tilining imkoniyatlari, zamonaviy kriptografik kutubxonalar, shifrlash va deshifrlash amaliyotlari, shuningdek, ushbu jarayonlar orqali axborotlarni samarali himoyalashning turli usullari ko‘rib chiqiladi. Shu bilan birga, axborot xavfsizligi muammolari va pythondan foydalangan holda ularni bartaraf etish uchun taqdim etiladigan yechimlar ham tahlil qilinadi[9-12].

Bugungi kunda axborot xavfsizligi bilan bog‘liq muammolar keng tarqalgan va turli ko‘rinishlarda namoyon bo‘lib kelmoqda masalan axborotning buzilishi, shaxsiy

ma'lumotlarni o‘g‘irlash, kompyuter viruslari va h.k. Bu muammolarni to‘g‘ri aniqlab, samarali yechimlar topish axborotlarni himoyalashda muhim ahamiyatga ega.

Python dasturlash tili axborot xavfsizligi muammolariga qarshi samarali yechimlarni tatbiq etishda muhim rol o‘ynaydi. Cryptography, PyCryptodome, hashlib kabi kutubxonalar yordamida zamonaviy kriptografik algoritmlarni qo‘llab, shifrlash, xeshlash, raqamli imzo yaratish va xavfsiz kommunikatsiyalarni ta'minlash imkonini beradi. Bu yechimlar axborot xavfsizligini ta'minlashda samarali himoya choralarini taqdim etadi[13-18].

Python dasturlash tili kriptografiya sohasida juda keng imkoniyatlar taqdim etadi. Ayniqsa, uning qulay va kuchli kutubxonalari orqali shifrlash algoritmlarini tatbiq etish oson va samaralidir. Bu borada eng ko‘p qo‘llaniladigan kutubxonalardan biri *cryptography* hisoblanadi. Ushbu kutubxona simmetrik va assimetrik shifrlashni qo‘llash uchun keng imkoniyatlar yaratadi. Simmetrik shifrlashda ma'lumotlarni shifrlash va deshifrlash uchun bitta kalit ishlatiladi. Ushbu usul tezkor va samarali bo‘lib, asosan katta hajmdagi ma'lumotlarni shifrlashda qo‘llaniladi va *cryptography* kutubxonasi orqali AES (Advanced Encryption Standard) kabi zamonaviy va kuchli shifrlash algoritmlarini ishlatish mumkin[18-22].

Simmetrik shifrlashning asosiy afzalligi shundaki, u nisbatan tez ishlaydi, lekin kalitni xavfsiz saqlash muammo bo‘lishi mumkin. Kalitni noto‘g‘ri qo‘llarga tushmasligi uchun maxsus xavfsizlik choralarini ko‘rish zarur.

Cryptography kutubxonasida simmetrik shifrlashdan foydalanish uchun quyidagicha kod yoziladi:

```
>>> from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes

>>> from cryptography.hazmat.backends import default_backend

>>> import os
```

```
# Kalit va boshlang'ich vektorni yaratish
>>> key = os.urandom(32)  # 256-bit AES kaliti
>>> iv = os.urandom(16)   # IV (Initialization Vector)
# Shifrlash uchun AES algoritmi va CBC rejimi
>>> cipher = Cipher(algorithms.AES(key), modes.CBC(iv), backend=default_backend())
>>> encryptor = cipher.encryptor()
>>> ct = encryptor.update(b"Bu maxfiy ma'lumot") + encryptor.finalize()
>>> print(ct)  # Shifrlangan ma'lumot
```

Yuqoridagi kodda *AES* algoritmi va *CBC* rejimi qo‘llanilgan. Bu ma'lumotlarni simmetrik tarzda shifrlash va deshifrlashda foydalaniladigan tez va xavfsiz usul hisoblanadi.

Python dasturlash tilidagi hashlib kutubxonasi kriptografik xeshlash funksiyalarini amalga oshirish uchun keng qo‘llaniladi. Xeshlash — bu ma'lumotlarni o'zgarmas uzunlikdagi "xesh" deb nomlangan qisqacha qiymatga aylantirish jarayoni. Xesh funksiyalari ma'lumotlarning yaxlitligini ta'minlash, ruxsatsiz o‘zgartirishlarni aniqlash va parollarni saqlashda keng qo‘llaniladi. Hashlib kutubxonasi turli xil xesh algoritmlarini taqdim etadi, jumladan:

SHA-256 (Secure Hash Algorithm 256-bit): Hozirgi kunda eng ko‘p qo‘llaniladigan xesh algoritmlaridan biri bo‘lib, 256 bit uzunlikdagi xavfsiz xesh qiymatini hosil qiladi.

SHA-1: Eskirgan, lekin ba'zi hollarda hali ham ishlatiladigan algoritm. Bu algoritm xavfsizlik nuqtai nazaridan zaifroq.

MD5: Tezkor, lekin hozirda kriptografik maqsadlar uchun tavsiya etilmaydi, chunki u zaif hisoblanadi.

Quyidagi misolda *SHA-256* algoritmi yordamida ma'lumotlarni qanday xeshlash ko'rsatiladi:

```
>>> import hashlib
# Xesh qilish uchun ma'lumot
>>> data = "Bu maxfiy ma'lumot".encode()  # Ma'lumotni baytlarga aylantirish
# SHA-256 algoritmidan foydalanib xeshlash
>>> hash_object = hashlib.sha256(data)
>>> hash_hex = hash_object.hexdigest()  # Xeshning o'n oltilik ko'rinishdagi shakli
>>> print(hash_hex)  # Xeshlangan qiymat
```

Yuqoridagi kodda: *"Bu maxfiy ma'lumot"* satri *SHA-256* algoritmi yordamida xeshlanadi va *hash_object.hexdigest()* funksiyasi xeshning o‘n oltilik shakldagi ko‘rinishini hosil qiladi. Bu natijada 64 belgidan iborat (256-bit) xesh qiymati olinadi.

PyCryptodome kutubxonasi python dasturlash tilida kriptografiya bo‘yicha qulay va kuchli vosita hisoblanadi. Ushbu kutubxona turli xil kriptografik algoritmlarni, jumladan, AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) va DSA (Digital Signature Algorithm) kabi algoritmlarni qo‘llab-quvvatlaydi. Keling, ushbu algoritmlar bilan ishlashni qanday amalga oshirishni ko‘rib chiqamiz.

AES — bu simmetrik shifrlash algoritmi bo‘lib, ma'lumotlarni shifrlash va deshifrlashda bitta kalitdan foydalanadi. *PyCryptodome* kutubxonasi yordamida AES algoritmini qo‘llash juda oson. AES bilan ishlash misoli:

```
>>> from Crypto.Cipher import AES
>>> from Crypto.Util.Padding import pad, unpad
```

```
>>> import os
# Kalit va boshlang'ich vektorni yaratish
>>> key = os.urandom(16)  # 128-bit kalit
>>> iv = os.urandom(16)   # 16 baytlik IV
# Ma'lumot
>>> data = b"Bu maxfiy ma'lumot"
# AES shifrlash
>>> cipher = AES.new(key, AES.MODE_CBC, iv)
>>> ciphertext = cipher.encrypt(pad(data, AES.block_size))
>>> print("Shifrlangan ma'lumot:", ciphertext)
# AES deshifrlash
>>> cipher = AES.new(key, AES.MODE_CBC, iv)
>>> decrypted_data = unpad(cipher.decrypt(ciphertext), AES.block_size)
>>> print("Deshifrlangan ma'lumot:", decrypted_data.decode())
```

Yuqoridagi kodda: AES algoritmi yordamida ma'lumot shifrlanadi va deshifrlanadi.

pad funksiyasi ma'lumotni bloklarga bo‘lishda foydalaniladi va *unpad* funksiyasi esa deshifrlash jarayonida olingan ma'lumotni tozalash uchun ishlatiladi.

RSA — bu assimetrik shifrlash algoritmi bo‘lib, ochiq va yopiq kalitlardan foydalanadi. Bu algoritm ma'lumotlarni shifrlashda va raqamli imzolarni yaratishda qo‘llaniladi. RSA bilan ishlash misoli:

```
>>> from Crypto.PublicKey import RSA
>>> from Crypto.Cipher import PKCS1_OAEP
# RSA kalitlarini yaratish
>>> key = RSA.generate(2048)
>>> private_key = key.export_key()
>>> public_key = key.publickey().export_key()
```

```
>>> print("Ochiq kalit:", public_key.decode())
# Ochiq kalit yordamida shifrlash
>>> cipher = PKCS1_OAEP.new(RSA.import_key(public_key))
>>> ciphertext = cipher.encrypt(b"Bu maxfiy xabar")
>>> print("Shifrlangan xabar:", ciphertext)
# Yopiq kalit yordamida deshifrlash
>>> cipher = PKCS1_OAEP.new(RSA.import_key(private_key))
>>> decrypted_data = cipher.decrypt(ciphertext)
>>> print("Deshifrlangan xabar:", decrypted_data.decode())
```

Bu yerda: RSA kalitlari yaratiladi va ochiq kalit yordamida ma'lumot shifrlanadi. Yopiq kalit yordamida shifrlangan ma'lumot deshifrlanadi.

Xulosa.

Ushbu maqolada axborotlarni himoyalashda Python dasturlash tilining imkoniyatlari, xususan, kriptografiya sohasida qanday foydali usullar va vositalar mavjudligi ko‘rib chiqildi. Zamonaviy raqamli dunyoda axborot xavfsizligi muammolari doimiy ravishda o‘sib bormoqda va ular turli ko‘rinishlarda namoyon bo‘layotganligi sababli, xavfsizlikni ta'minlash uchun innovatsion yechimlar zarur. Python dasturlash tili va uning kuchli kutubxonalari, xususan, *cryptography*, *hashlib*, va *PyCryptodome*, ushbu muammolarni hal qilishda muhim ahamiyatga ega. Maqolada ko‘rib chiqilgan shifrlash, xeshlash va raqamli imzo yaratish usullari, axborotlarni himoya qilishda ishonchli vositalar sifatida xizmat qiladi. AES algoritmi yordamida ma'lumotlar xavfsiz ravishda shifrlanadi, RSA yordamida esa ma'lumotlarni shifrlash va imzolash jarayonlari amalga oshiriladi. DSA algoritmi esa raqamli imzolarni yaratishda va ularning to‘g‘riligini tekshirishda muhim rol o‘ynaydi. Pythonning soddaligi va kuchli kutubxonalari yordamida kriptografik jarayonlarni oson va

samarali tarzda amalga oshirish mumkin. Bu dasturchilarga zamonaviy xavfsizlik talablariga mos keladigan yechimlarni ishlab chiqishda katta yordam beradi. Shuningdek, bu maqsadlarda muhim bo‘lgan vositalar orqali kriptografiya sohasida doimiy yangiliklar va rivojlanishlar mavjud. Python dasturlash tili axborot xavfsizligi muammolarini hal qilishda muhim rol o‘ynaydi. Uning kuchli kutubxonalari orqali kriptografiya amaliyotlarini amalga oshirish oson va ishonchli bo‘lib, bu zamonaviy raqamli dunyoda axborotlarni himoya qilishda eng samarali vositalardan biridir. Shunday qilib, Python va kriptografiya birgalikda axborotlarni himoyalashning asosiy poydevorini tashkil etadi va bu sohada yanada rivojlanishga katta imkoniyatlar yaratadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Rakhmatullaev I. Evaluation of new NSA stream encryption algorithm by integrated cryptanalysis method //Scientific Collection «InterConf». – 2023. – №. 164. – С. 242-248.

2. Raxmatullayebich R. I. STREAM ENCRYPTION ALGORITHMS AND THE BASIS OF THEIR CREATION //Central asian journal of mathematical theory and computer sciences. – 2022. – Т. 3. – №. 12. – С. 165-173.

3. Khudoykulov Z. T., Rakhmatullaev I. R., Umurzakov O. S. H. NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o ‘rni //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – Т. 6. – №. 4. – С. 97-101.

4. Xudoyqulov Z. T., Rahmatullayev I. R., Boyqo‘ziyev I. M. Bardoshli statik S-bokslarni generatsiyalash algoritmi //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – Т. 5. – №. 3. – С. 57-66.

5. Rakhmatullaev I. Self-synchronizing (asynchronous) Stream Encryption Algorithms //Scientific Collection «InterConf». – 2023. – №. 164. – С. 249-254.

6. Zaynalov N. R. et al. Classification and ways of development of text steganography methods //ISJ Theor Appl Sci. – 2019. – Т. 10. – №. 78. – С. 228-232.

7. Boyquziyev I., Saydullayev E., Rahmatullayev I. ELLIPTIK EGRI CHIZIQLARNING KRIPTOGRAFIYADA QO ‘LLANILISHI //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 1. – С. 71-76.

8. Rahmatullayev I. R. Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo‘llanish asoslari: Algebraic Cryptanalysis Method and Basics of its Application to Stream Encryption Algorithm //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2023. – Т. 4. – №. 2. – С. 96-102.

9. Xudoykulov Z. T., Rahmatullayev I. R. Yangi oqimli shifrlash algoritmlari va uning kriptotahlili //Milliy standart Ilmiy-texnik jurnali. – 2023. – С. 42-47.

10. Rahmatullayev I. R. Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2022. – Т. 2. – №. 2. – С. 119-128.

11. Zaynalov N. R. et al. UNICODE For Hiding Information In A Text Document //2020 IEEE 14th International Conference on Application of Information and Communication Technologies (AICT). – IEEE, 2020. – С. 1-5.

12. Rahmatullayev I., Xudoyqulov Z. T. Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili tahlili //Потомки Аль-Фаргани. – 2024. – Т. 1. – №. 1. – С. 129-134.

13. Kilichev D. et al. Errors in SMS to hide short messages //Artificial Intelligence, Blockchain, Computing and Security Volume 2. – CRC Press, 2024. – С. 735-740.

14. Rahmatullayev I., Umurzakov O. SHA oilasiga mansub xesh funksiyalar tahlili //Потомки Аль-Фаргани. – 2024. – Т. 1. – №. 1. – С. 85-92.

15. Rahmatullayev I. R., Saydullayev E. I., Karimov I. KRIPTOGRAFIYADA ELLIPTIK EGRI CHIZIQLARNING AHAMIYATI //Talqin va tadqiqotlar. – 2024. – №. 28.

16. Rahmatullayev I. et al. OQIMLI SHIFRLASH ALGORITMLARINING LOYIHALASH USULLARI //Talqin va tadqiqotlar. – 2024. – Т. 1. – №. 27.

17. Rakhmatullaevich R. I., Mardanokulovich I. B. Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2024. – С. 393-401.

18. Rahmatullayev I., Karimov I. DASTURIY SHAKLDA FOYDALANISHGA QULAY OQIMLI SHIFRLASH ALGORTIMINI ISHLAB CHIQISH //Talqin va tadqiqotlar. – 2024. – №. 5 (42).

19. Rahmatullayev I. et al. OQIMLI SHIFRLAR VA ULARNI KRIPTOGRAFIYADAGI O ‘RNI //Interpretation and researches. – 2024. – Т. 2. – №. 3 (25).

20. Rahmatullayev I. OQIMLI SHIFRLASH ALGORITMLARI BARDOSHLILIGINI DIFFERENSIAL VA ALGEBRAIK KRIPTOTAHLIL USULLARI YORDAMIDA BAHOLASH //DIGITAL TRANSFORMATION AND ARTIFICIAL INTELLIGENCE. – 2024. – Т. 2. – №. 1. – С. 64-70.

21. Khudoykulov Z. T., Rakhmatullayev I. R. Development Of A Software Stream Encryption Algorithm //Electronic journal of actual problems of modern science, education and training. – 2023. – Т. 1. – С. 51-59.

22. Raxmatullayevich R. I. OQIMLI SHIFRLASH ALGORITMLARI TAHLILI //Новости образования: исследование в XXI веке. – 2023. – Т. 1. – №. 6. – С. 889-893.