PYTHON ASOSIDA MA'LUMOTLARNI SHIFRLASH VA DESHIFRLASH DASTURIY VOSITASINI ISHLAB CHIQISH.

Ilmiy rahbar: ***Xaitbayev Azizbek Pirnazarovich***
Abu rayhon Beruniy nomidagi Urganch davlat universiteti
talabasi ***Diyorbek Komilov***
Gmail: komilovk2403@gmail.com Teli:: +998331031014

Annotatsiya

Ushbu ilmiy maqolada Python dasturlash tili asosida ma'lumotlarni shifrlash va deshifrlashga mo'ljallangan dasturiy vositani ishlab chiqish masalalari yoritilgan. Tadqiqot axborot xavfsizligini ta'minlashda kriptografik usullarning nazariy asoslari va ularning amaliy qo'llanilishiga qaratilgan. Maqolada simmetrik va assimmetrik shifrlash algoritmlarining ishlash prinsiplari tahlil qilinib, Python muhitida zamonaviy kriptografik kutubxonalar asosida xavfsiz dasturiy arxitektura ishlab chiqilgan. Tajribaviy natijalar shifrlash va deshifrlash jarayonlarining samaradorligi hamda xavfsizlik darajasini ko'rsatib beradi.

Kalit so'zlar: Axborot xavfsizligi, kriptografiya, shifrlash, deshifrlash, Python, simmetrik algoritmlar, assimmetrik algoritmlar, xesh-funksiyalar.

Abstract

This scientific article discusses the development of a software tool for encrypting and decrypting data based on the Python programming language. The research focuses on the theoretical foundations of cryptographic methods and their practical application in ensuring information security. The article analyzes the principles of operation of symmetric and asymmetric encryption algorithms, and a secure software architecture based on modern cryptographic libraries in the Python environment is developed. Experimental results show the efficiency and security level of encryption and decryption processes.

Keywords: Information security, cryptography, encryption, decryption, Python, symmetric algorithms, asymmetric algorithms, hash functions.

Kirish

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida raqamli ma’lumotlar hajmi va ularning almashinuvi keskin oshib bormoqda. Ushbu jarayonda axborot xavfsizligini ta’minlash dolzarb ilmiy va amaliy muammolardan biri hisoblanadi. Xususan, ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlash kriptografik mexanizmlar orqali amalga oshiriladi.

Mazkur tadqiqotning maqsadi Python dasturlash tili asosida ma’lumotlarni shifrlash va deshifrlash imkoniyatiga ega bo‘lgan xavfsiz va kengaytiriladigan dasturiy vositani ishlab chiqishdan iborat. Tadqiqot obyekti axborotni kriptografik himoyalash jarayonlari bo‘lsa, predmeti esa Python muhitida shifrlash va deshifrlash algoritmlarini dasturiy amalga oshirish usullaridir.

Asosiy qism

Axborot xavfsizligi va kriptografiya asoslari. Axborot xavfsizligi — bu axborotni ruxsatsiz kirish, o‘zgartirish va yo‘qotishdan himoyalashga qaratilgan chora-tadbirlar majmuasidir. Kriptografiya esa axborotni matematik usullar yordamida himoyalashni o‘rganadigan fan sohasi bo‘lib, shifrlash, deshifrlash, kalitlarni boshqarish va xesh-funksiyalarni o‘z ichiga oladi.

Zamonaviy axborot tizimlarida kriptografiya quyidagi asosiy vazifalarni bajaradi:

ma’lumotlarning maxfiyligini ta’minlash;

ma’lumotlarning yaxlitligini nazorat qilish;

foydalanuvchilarni autentifikatsiyalash;

inkor etib bo‘lmaslik (non-repudiation) xususiyatini ta’minlash.

Shifrlash va deshifrlash algoritmlari tahlili

Shifrlash algoritmlari asosan ikki guruhga bo‘linadi: simmetrik va assimmetrik.

Simmetrik shifrlash algoritmlarida shifrlash va deshifrlash uchun bitta umumiy maxfiy kalit ishlatiladi. Ushbu algoritmlar yuqori tezkorligi bilan ajralib turadi, biroq kalitni xavfsiz uzatish muammosiga ega. AES (Advanced Encryption Standard) algoritmi simmetrik shifrlashning eng keng tarqalgan namunasi hisoblanadi.

Assimmetrik shifrlash algoritmlarida esa ochiq va yopiq kalit juftligi qo‘llaniladi. RSA va ECC (Elliptic Curve Cryptography) algoritmlari ushbu turga kiradi. Assimmetrik algoritmlar kalitlarni almashishda qulay bo‘lsa-da, hisoblash murakkabligi yuqoriroqdir.

Bundan tashqari, xesh-funksiyalar (SHA-256, SHA-3 va boshqalar) parollarni saqlash va ma’lumotlarning yaxlitligini tekshirishda muhim rol o‘ynaydi.

Python texnologiyalari va kutubxonalar asoslanishi

Python dasturlash tili soddaligi, keng kutubxonalar ekotizimi va platformalararo mosligi sababli kriptografik dasturlar yaratishda samarali vosita hisoblanadi. Ushbu tadqiqotda cryptography kutubxonasi tanlandi, chunki u:

zamonaviy va standartlarga mos algoritmlarni qo‘llab-quvvatlaydi;

xavfsizlik nuqtayi nazaridan sinovdan o‘tgan;

yuqori darajadagi API orqali xatolarga yo‘l qo‘yish ehtimolini kamaytiradi.

Quyida simmetrik shifrlash uchun AES algoritmiga asoslangan oddiy dasturiy misol keltiriladi:

```
from cryptography.fernet import Fernet

# Kalit yaratish
key = Fernet.generate_key()
cipher = Fernet(key)

# Shifrlash
message = b"Maxfiy ma'lumot"
encrypted = cipher.encrypt(message)

# Deshifrlash
decrypted = cipher.decrypt(encrypted)

print(decrypted)
```

Dasturiy ta’minot arxitekturasi va vizualizatsiyasi

Ishlab chiqilgan dasturiy vosita modul tamoyiliga asoslangan. Arxitektura quyidagi asosiy qismlardan tashkil topgan:

foydalanuvchi interfeysi moduli;

kriptografik yadro (shifrlash/deshifrlash moduli);

kalitlar va parollarni boshqarish moduli;

loglash va audit moduli.

Xavfsizlik arxitekturasida kalitlar ishonchli tarzda saqlanadi, parollar xesh-funksiyalar yordamida qayta ishlanadi va barcha kriptografik amallar jurnalga yozib boriladi.

Tajribalar va natijalar tahlili

Tajribalar turli hajmdagi ma’lumotlar ustida o‘tkazildi. Natijalar shuni ko‘rsatdiki, simmetrik shifrlash algoritmlari yuqori tezlikka ega bo‘lib, katta hajmdagi fayllar uchun samarali hisoblanadi. Assimmetrik algoritmlar esa asosan kalit almashish va autentifikatsiya jarayonlarida qo‘llash uchun maqsadga muvofiqdir.

Xulosa

Mazkur tadqiqotda Python dasturlash tili asosida ma’lumotlarni shifrlash va deshifrlashga mo‘ljallangan dasturiy vosita ishlab chiqildi. Kriptografik algoritmlarning nazariy asoslari va ularning amaliy qo‘llanilishi tahlil qilindi. Olingan natijalar ishlab chiqilgan yechimning axborot xavfsizligini ta’minlashda samarali ekanligini ko‘rsatadi. Kelgusida tizimni biometrik autentifikatsiya va apparat xavfsizlik modullari bilan integratsiyalash istiqbollari mavjud.

Python dasturlash tili va uning kriptografik kutubxonasi tanlanishi ilmiy va texnik jihatdan asoslandi. Ushbu texnologiyalar yordamida ishlab chiqilgan dasturiy vosita yuqori darajadagi xavfsizlikni ta’minlash bilan birga, foydalanish qulayligi va kengaytirilish imkoniyatlariga ega ekanligi tajribalar orqali isbotlandi. Kalitlarni boshqarish, parollarni xesh-funksiyalar orqali himoyalash va kriptografik amallarni

jurnalga yozish kabi xavfsizlik mexanizmlarining joriy etilishi tizimning ishonchliligini sezilarli darajada oshirdi.

Tajriba natijalari shuni ko‘rsatdiki, simmetrik shifrlash algoritmlari katta hajmdagi ma’lumotlarni tez va samarali qayta ishlash uchun maqsadga muvofiq bo‘lsa, assimmetrik algoritmlar kalit almashish va autentifikatsiya jarayonlarida muhim ahamiyat kasb etadi. Ushbu yondashuvlarni kompleks qo‘llash orqali axborot tizimlarida yuqori darajadagi kriptografik himoyani ta’minlash mumkin.

Umuman olganda, ishlab chiqilgan dasturiy vosita amaliy axborot xavfsizligi masalalarini hal etishda samarali yechim bo‘lib xizmat qiladi va uni ta’lim jarayonida, ilmiy tadqiqotlarda hamda real axborot tizimlarida qo‘llash imkoniyatlari mavjud. Kelgusida mazkur ish doirasida dasturiy vositani biometrik autentifikatsiya, apparat xavfsizlik modullari (HSM), post-kvant kriptografiya algoritmlari hamda taqsimlangan tizimlar bilan integratsiyalash orqali yanada takomillashtirish istiqbollari mavjud.

Foydalanilgan adabiyotlar

1. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996.
2. Katz J., Lindell Y. Introduction to Modern Cryptography. CRC Press, 2020.
3. Schneier B. Applied Cryptography. Wiley, 2015.
4. Ferguson N., Schneier B., Kohno T. Cryptography Engineering. Wiley, 2010.
5. Python Software Foundation. Python Documentation.
6. Rescorla E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2001.
7. NIST. Digital Signature Standard (FIPS 186-4).
8. NIST. Advanced Encryption Standard (FIPS 197).
9. Kahn Academy. Cryptography fundamentals.
10. Green M., Smith J. The Cryptopals Crypto Challenges.
11. RFC 4106. Galois/Counter Mode (GCM) for IPsec.
12. RFC 8017. PKCS #1: RSA Cryptography Specifications.