Acumen: International Journal of Multidisciplinary Research
ISSN: 3060-4745 IF(Impact Factor)10.41 / 2024
Volume 2, Issue 4

MILLIY KRIPTOGRAFIK ALGORITMLAR ASOSIDA DASTURIY KUTUBXONA ARXITEKTURASINI ISHLAB CHIQISH VA BAHOLASH

Boboyeva Fotimaxon Abdumurot qizi
Termiz davlat universiteti magistranti

Annotatsiya: Mazkur maqolada milliy kriptografik algoritmlarning xususiyatlari va ularning asosida samarali, xavfsiz va kengaytiriluvchi kriptografik kutubxona arxitekturasini ishlab chiqish masalalari yoritilgan. Tadqiqotda O‘zbekiston Respublikasida amalda mavjud bo‘lgan O‘zDSt shifrlash standartlari tahlil qilinadi va ushbu algoritmlarni qo‘llovchi modulli dasturiy kutubxona taklif etiladi. Arxitektura komponentlari, funksional modul strukturalari hamda xavfsizlik darajasi zamonaviy xalqaro standartlar bilan taqqoslab baholanadi. Shuningdek, kutubxonaning potensial amaliy qo‘llanilish sohasi, ayniqsa elektron hukumat va moliyaviy xizmatlar xavfsizligi kontekstida ko‘rib chiqiladi.

Kalit so‘zlar: milliy kriptografiya, dasturiy kutubxona, O‘zDSt algoritmlari, raqamli imzo, xavfsizlik arxitekturasi, modullilik, OpenSSL integratsiyasi.

KIRISH

Axborot xavfsizligini ta’minlashda kriptografik algoritmlarning o‘rni beqiyos. Har bir davlat o‘zining xavfsizlik siyosatiga muvofiq milliy standartlarga asoslangan algoritmlarni ishlab chiqadi. O‘zbekistonda ham O‘zDSt 1105:2009, O‘zDSt 1106:2009 va boshqa standartlar asosida milliy kriptografik algoritmlar mavjud. Shu bilan birga, ushbu algoritmlarni dasturiy ta'minot shaklida keng ko‘lamda qo‘llash uchun mos kutubxona arxitekturasini yaratish dolzarb masalalardan biridir.

ILMIY ASOSLAR VA TADQIQOT HOLATI

Ko‘plab xalqaro tadqiqotlarda (Stallings, Schneier, Menezes) kriptografik tizimlarning mustahkamligi, modulliligi va xavfsizlik darajasi haqida fikr yuritilgan. O‘zbekiston sharoitida esa O‘zDSt standartlariga asoslangan tizimlar, ko‘proq yopiq muhitlarda qo‘llanilib, ularning ochiq, kengaytiriluvchi arxitekturasi hali to‘liq shakllantirilmagan.

Acumen: International Journal of Multidisciplinary Research
ISSN: 3060-4745 IF(Impact Factor)10.41 / 2024
Volume 2, Issue 4

KUTUBXONA ARXITEKTURASI LOYIHASI

Taklif etilayotgan kutubxona quyidagi modullardan iborat:

- **Core module** – shifrlash va deshifrlash funksiyalarini bajaradi.
- **Hashing module** – O‘zDSt 1106:2009 algoritmi asosida xesh hisoblash.
- **Signature module** – raqamli imzo yaratish va tekshirish.
- **Key generation module** – kalit generatsiyasi.
- **Integration module** – OpenSSL, Python, C++ bilan integratsiya imkoniyati.

Arxitektura **mikroxizmatlar printsipida** qurilib, har bir modul mustaqil ravishda test qilinadi va yangilanadi.

ARXITEKTURA USTUNLIKLARI

- Milliy standartlarga to‘liq moslik
- Ochiqlik va kengaytiriluvchanlik
- Ko‘p tillilik (API for Python, C++, Rust)
- Platformalarga moslik (Linux, Windows, Embedded systems)

TAQQOSLI TAHLIL

Mezoni	**OpenSSL**	**Taklif etilgan kutubxona**
Milliy algoritmlar	Qo‘llamaydi	To‘liq qo‘llaydi
Moslashuvchanlik	Yuqori	Yuqori
Xavfsizlik	Yuqori	Yuqori
Tillar bilan API	C, Python	C++, Python, Rust

XULOSA

Milliy kriptografik algoritmlarga asoslangan kutubxona arxitekturasini yaratish O‘zbekiston axborot xavfsizligini mustahkamlashda muhim ahamiyatga ega. Taklif etilgan kutubxona arxitekturasi ochiqlik, modullilik va xalqaro integratsiyaga tayyorlik kabi afzalliklari bilan ajralib turadi.

FOYDALANILGAN ADABIYOTLAR

1. Schneier, B. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley & Sons.
2. Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice*. 7th Edition. Pearson Education.
3. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
4. OpenSSL Project. (2024). *OpenSSL Cryptography and SSL/TLS Toolkit*. https://www.openssl.org
5. O‘zbekiston Respublikasi Standartlashtirish, metrologiya va sertifikatlashtirish agentligi. (2009). *O‘zDSt 1105:2009 — Ma'lumotlarni shifrlash algoritmi*.
6. O‘zbekiston Respublikasi Standartlashtirish, metrologiya va sertifikatlashtirish agentligi. (2009). *O‘zDSt 1106:2009 — Xesh funksiyasi*.
7. O‘zbekiston Respublikasi Standartlashtirish, metrologiya va sertifikatlashtirish agentligi. (2009). *O‘zDSt 1092:2009 — Elektron raqamli imzo: Yaratish va tekshirish*.
8. O‘zbekiston Respublikasi Standartlashtirish, metrologiya va sertifikatlashtirish agentligi. (2014). *O‘zDSt 2826:2014 — Axborotni himoyalash. Raqamli imzo algoritmlari*.
9. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
10. Koblitz, N. (1987). *Elliptic curve cryptosystems*. Mathematics of Computation, 48(177), 203–209.