AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH VOSITALARI VA ULARNI AMALIYOTDA QO‘LLASH USULLARI

Mo‘minov Anvarjon To‘lqinjon o‘g‘li
Sodiqov Boburmirzo Sobitjon o‘g‘li
Toshkent Axborot Texnologiyalari Universiteti
Farg`ona filiali talabasi

Annotatsiya: Kriptografiya, axborotlarni himoyalash uchun ishlatiladigan texnologiyalarning umumiy nomidir. Bu texnologiyalar axborotni to'g'ridan-to'g'ri o'qib olish, o'zgartirish va boshqa hodisalardan himoyalashni ta'minlash uchun foydalaniladi.

Kalit so'zlar: Shifrlash, dekodlash, des algoritmi, aes enkripsiya, blok shifrlash, chiq kalit, maxfiy kalit, rsa algoritmi, kalit almashinuvi, elektron imza, kriptoalgoritm.

"Axborotlarni kriptografik himoyalash vositalari" deyilganida, siz mazkur axborotlarni (ma'lumotlar) himoyalash uchun foydalaniladigan kriptografik protokollar, algoritmlar va vositalar haqida so'zlashmoqdasiz. Kriptografiya, axborotlarni himoyalashda ishlatiladigan texnologiyalarni tushunish va ulardan foydalanishga yordam beradi.

Kriptografik Himoyalash Vositalari: Bu qismda kriptografik himoyalash vositalari, shu jumladan shifrlovka algoritmlari, imzolash protokollari, hashlash algoritmlari, va boshqa tizimlar haqida tafsilotlar beriladi. AES, RSA, va SHA-256 kabi kriptografik algoritmlar haqida ma'lumotlar ham shu jumladan ko'rsatiladi.

Multi-Factor Authentication (MFA) va Zero-Knowledge Proof: Kriptografik himoyalashni kuchaytirish uchun foydalaniladigan yana bir qator vositalar MFA va Zero-Knowledge Proof bo'lib, ularning ahamiyati, ishlash prinsiplari va qo'llanish sohalariga oid ma'lumotlar ko'rsatiladi.

Side-Channel Attacks va Kvant Kriptografiyasi: Hujumchilar tarafidan amalga oshiriladigan turlardan himoyalashda muhofazalash uchun maqolada Side-Channel Attacks va Kvant Kriptografiyasi mavzulariga oid ma'lumotlar keltirilib, ularni oldini olish uchun kerakli himoyalash vositalarining muhimligi ta'kidlanadi.

Tendentsiyalar va Yangi Texnologiyalar: Maqola oxiriga yaqinlashgan qismda, kriptografik himoyalash sohasidagi so'nggi tendentsiyalar, yangi texnologiyalar, va kelajakdagi rivojlanishlarga oid proqnozlar muhokama qilinadi. Bu qismda,

blockchain texnologiyasi, homomorphic encryption, va quantum-resistant kriptografiyani ko'rsatish mumkin.

Quyidagi kriptografik himoyalash vositalari va ulardan ishlatishning ba'zi misollarini ko'rsatish mumkin:

Shifrlovka (Encryption):

Algoritmlar: AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), DES (Data Encryption Standard), ChaCha20, va boshqa.

Protokollar: TLS (Transport Layer Security), IPSec (Internet Protocol Security).

Imzolash (Digital Signatures):

Algoritmlar: RSA, ECDSA (Elliptic Curve Digital Signature Algorithm).

Protokollar: PGP (Pretty Good Privacy), S/MIME (Secure/Multipurpose Internet Mail Extensions).

Hashlash (Hashing):

Algoritmlar: SHA-256, SHA-3, MD5 (boshqacha tahlil etiladi).

Ishlatish misollar: Parollar va ma'lumotlar taminlash, ma'lumotlarning integritetini tekshirish.

Kripto-valyuta: Blockchain texnologiyasi, kripto-valyuta uchun kriptografik himoya vositalarini ishlatadi. Misol uchun, Bitcoin-da SHA-256 hashing algoritmi va ECDSA imzolash algoritmi ishlatiladi.

Public Key Infrastructure (PKI):

Asosiy qismi: Aloqada bo'lgan o'zgarishlarni kuzatish va havolalarni amalga oshirish uchun ishlatiladi.

Vositalar: X.509 sertifikatlari, Certification Authorities (CA).

Multi-Factor Authentication (MFA):

Tushunchalar: Bu usul, foydalanuvchining identifikatsiyasini amalga oshirishda bir nechta turdagi ma'lumotlarni (faktorlarni) ishlatadi.

Misollar: Parol, SMS-kod, biometrik identifikatsiya (qo'l izi, yuz tanishuvi), taqrizli kodi olish uchun ilova.

Zero-Knowledge Proof:

Tushuncha: Bu usulda, bir tomonda bo'lgan ma'lumotlar yuboriladigan tomonning ma'lumotlari to'liq nol bilan sabablanadi.

Foydalanish sohalar: Endi qonun korxonalari, kripto-valyuta platformalari.

Homomorphic Encryption:

Tushuncha: Ma'lumotlar shifrlangan holda qoladi, va hisob-kitob amaliyotlarni shifrlangan ma'lumotlar ustida bajarish mumkin.

Foydalanish sohalar: Cloud computing, ma'lumotlar bazalari.

Side-Channel Attacks ni qo'llash:

Tushuncha: Hujumchilar ma'lumotlarni kuzatish uchun qurilmalarning qo'shimcha kanallaridan foydalanishadi.

Sirtqichlar: Fiziksel tamonlama, zaryad so'ralganligi, elektromagnit so'ralganligi.

Kvant Kriptografiyasi:

Tushuncha: Ma'lumotlar kuzatilganda, kubitlar (kvant xossalari) ustida amal qilingan hujumni aniqlash uchun texnologiya.

Potentsial foydalash sohalar: Internet of Things (IoT), kripto-valyutalar.

Kriptografik himoyalash vositalari va protokollarining qo'shimcha yaxshi tushuniladigan va yuqori sifatli bo'lishi uchun, ulardagi hujumlar va yanada yaxshi hisob-kitob qilish uchun yangi texnologiyalar va usullar ham ishlab chiqilmoqda. Bu sohada davom etadigan ilovalar va texnologiyalar takomillashtirilgan kuzatib borilmoqda.

Kriptografik himoyalash vositalari, axborotlar uchun himoya tizimini amalga oshirishda yaxshi natijalarni ko'rsatadi. Biroq, bu vositalarni ishlatishda va xizmatni o'rnatishda, mahsulot tuzilmasining eng yangi xavf va taqiqlovlarini kuzatib borish kerak.

Foydalanilgan adabiyotlar:

1. Turgunova, N., Turgunov, B., & Umaraliyev, J. (2023). AUTOMATIC TEXT ANALYSIS. SYNTAX AND SEMANTIC ANALYSIS. *Engineering problems and innovations*.
2. Turg‘unov, B., Turg‘unova, N., & Umaraliyev, J. (2023). AVTOMOBILSOZLIKDA AVTOMATLASHTIRISHNING O ‘RNI. *Engineering problems and innovations*.
3. Nafisaxon, T. U., Jamshidbek To‘xtasin o‘g, U., Arsenevna, D. E., & Azimjon o‘g‘li, A. O. (2022). AVTOMATLASHTIRILGAN AVTOTURARGOH IMKONIYATLARI VA QULAYLIKLARI. *INNOVATION IN THE MODERN EDUCATION SYSTEM*, *3*(25), 45-48.