SHIFRLASH STANDARTLARI

Po’latov Doston Normurod o’g’li
Yoqubova Madinabonu Abdushukur qizi
Torebaeva Naziyra
Shonazarov Sarvarbek Maqsud o‘g‘li

Annotatsiya: *Shifrlash standartlari, ma'lumotlarni shifrlash, de-shifrlash, autentifikatsiya qilish va himoya qilishning standart protokollari va algoritmlari to'plamidir. Ularning asosiy maqsadi konfidensiallikni ta'minlash, ma'lumotlarni himoya qilish va integritetni ta'minlashdir.*

Shifrlash standartlari bir nechta komponentlardan iborat bo'lishi mumkin:

1. Kalitlar: Shifrlashda kalitlar, ma'lumotlarni shifrlash va de-shifrlash uchun kerak bo'lgan maxfiy bilan bir xil qiymatdagi elementlar hisoblanadi. Kalitlar, shifrlash algoritmlari tomonidan ishlatiladi va ma'lumotlarni himoya qilishning asosiy faktori hisoblanadi.

2. Shifrlash algoritmlari: Shifrlash standartlarida foydalaniladigan shifrlash algoritmlari, ma'lumotlarni shifrlash va de-shifrlash operatsiyalarini amalga oshirish uchun ishlatiladigan matematik formulalar va protseduralar to'plami hisoblanadi. Bu algoritmlar, kalitlar bilan birgalikda foydalaniladi va ma'lumotlarni shifrlash va de-shifrlash jarayonlarini bajarish uchun xavfsizlik va to'g'rilikni ta'minlashda muhim rol o'ynayadi.

3. Autentifikatsiya protokollari: Shifrlash standartlarida autentifikatsiya protokollari foydalanuvchilarning identifikatsiyasini va ma'lumotlarni to'g'ri va xavfsiz tarzda almashishni ta'minlash uchun ishlatiladi. Bu protokollar, foydalanuvchilarni autentifikatsiya qilish, kalitlarni almashtirish va ma'lumotlarni himoya qilishning to'g'ri tarzda amalga oshirilishini ta'minlash uchun berilgan yo'llarni o'z ichiga oladi.

4. Xeshlash protokollari: Xeshlash protokollari, ma'lumotlarni integritetni tekshirish va xavfsizlikni ta'minlash uchun foydalaniladi. Bu protokollar ma'lumotlar yordamida xesh qiymatlarini generatsiya qilish va tekshirish jarayonlarini o'z ichiga oladi. Xesh qiymatlari, ma'lumotlar o'zgartirilganligini aniqlash uchun ishlatiladi va ma'lumotlar to'g'risidagi o'zgarmaslikni ta'minlashda muhim rol o'ynayadi.

Kalit so’zlar: *shifrlash,De-shifrlash, maxfiy kalit, habar, Kalit.*

Abstract: *Encryption standards are a set of standard protocols and algorithms for data encryption, decryption, authentication, and protection. Their primary purpose is to ensure confidentiality, data protection and integrity.*

Encryption standards can consist of several components:

1. Keys: In encryption, keys are elements of the same value as the secret needed to encrypt and de-encrypt data. Keys are used by encryption algorithms and are a key factor in data protection.

2. Encryption algorithms: Encryption algorithms used in encryption standards are a set of mathematical formulas and procedures used to perform data encryption and decryption operations. These algorithms are used in conjunction with keys and play an important role in providing security and integrity to perform data encryption and de-encryption processes.

3. Authentication Protocols: In encryption standards, authentication protocols are used to ensure the identification of users and the correct and secure exchange of data. These protocols include ways to ensure that user authentication, key exchange, and data protection are properly implemented.

4. Hashing Protocols: Hashing protocols are used to check data integrity and ensure security. These protocols include the processes of generating and validating hash values using data. Hash values are used to determine whether data has been modified and play an important role in ensuring data integrity.

Keywords: *encryption, De-encryption, secret key, message, Key.*

KIRISH

Shifrlash standartlari, ma'lumotlarni xavfsiz tarzda almashish va himoya qilishning belgilangan protokollari va algoritmlaridir. Bu standartlar, ma'lumotlar ustida tashqi tomonlar tomonidan amalga oshirilishi mumkin bo'lgan hujjatlardan himoya qilishni ta'minlash uchun yaratilgan.

Shifrlash standartlari, quyidagi asosiy elementlardan iborat bo'lishi mumkin:

1. Shifrlash algoritmlari: Shifrlash standartlarida qo'llaniladigan ma'lumotlarni shifrlash va de-shifrlash uchun belgilangan matematik algoritmlari mavjud. Bu algoritmlar ma'lumotlarni kalitlar bilan o'zgartirish va undan so'ng ma'lumotni qaytarish uchun qo'llaniladi. Mashhur shifrlash algoritmlaridan ba'zilari DES (Data Encryption Standard), AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), va ECC (Elliptic Curve Cryptography) shifrlash algoritmlaridir.

2. Axborot izchillik protokollari: Shifrlash standartlari, ma'lumotlarni almashish va uzatish jarayonlarida axborot izchillik protokollari orqali foydalanishni ta'minlayadi. Bu protokollar, ma'lumotlarni shifrlab yuborish, qabul qilish, kimni autentifikatsiya qilish va ma'lumotlarning integralligini tekshirish imkonini beradi. Mashhur axborot izchillik protokollari SSL/TLS (Secure Sockets Layer/Transport Layer Security), IPSec (Internet Protocol Security) va SSH (Secure Shell) protokollari bilan bog'liq.

3. Kalit menedjmenti: Shifrlash standartlari, kalit menedjmenti prinsiplari va qoidalarini taqdim etadi. Bu, kalitli kalitlar yaratish, saqlash, tarqatish va boshqarish jarayonlarini ta'minlashni o'z ichiga oladi. Standartlar, kalitlar tuzish usullarini, kalitlarni uzatish va qabul qilishning xavfsiz yo'llarini va kalitlarni yangilash va tarqatishning protseduralarini belgilaydi.

Shifrlash standartlarining afzalliklari quyidagilardan iborat:

1. Xavfsizlik: Shifrlash standartlari ma'lumotlarni tashqi tomonlar tomonidan himoya qilishga yordam beradi. Ular, ma'lumotlar ustida amalga oshirilishi mumkin bo'lgan hujjatlardan himoya qilish, ma'lumotlarni maxfiy tarzda almashish va ularga faqatgina ruxsat etilgan odamlar tomonidan o'qish imkonini ta'minlash imkonini beradi.

2. Integritet: Shifrlash standartlari ma'lumotlarning o'zgartirilganligini aniqlash va himoya qilishga yordam beradi. Xesh qiymatlari va tekshiruvlar orqali ma'lumotlarning o'zgartirilganligini aniqlash imkonini ta'minlayadi.

3. Konfidensiallik: Shifrlash standartlari ma'lumotlarning maxfiylikni ta'minlashda muhim rol o'ynayadi. Ma'lumotlar shifrlangan holda saqlanadi va faqatgina kalitni biluvchi tomonidan de-shifrlash mumkin bo'ladi.

4. Interoperatsiya: Shifrlash standartlari ommaviy sifatda qo'llaniladi va ko'p tashqi tizim va dasturlarning ularga mos kelishini ta'minlayadi. Bu, turli platformalar, tizimlar va tahlilgarlar orasida ma'lumot almashishni osonlashtiradi.

Shifrlash standartlarining kamchiliklari quyidagilardan iborat bo'lishi mumkin:

1. So'nggi tekhnologiyalarni qo'llash: Shifrlash standartlari, so'nggi tekhnologiyalarni va to'g'ridan-to'g'ri tartiblangan xattacklar bilan to'g'ridan-to'g'ri kurashishga qodir bo'lishi kerak. Agar standartlar yangilanmasa, ular tomonidan himoya qilinayotgan ma'lumotlar haqida yangi xattacklar va kutilmagan kamchiliklar paydo bo'lishi mumkin.

2. Kompatibilitet: Shifrlash standartlari va protokollari odatda muayyan tizimlar va dasturlar bilan birgalikda ishlatiladi. Ular orasida kompatibilitetni ta'minlash, standartlarning yaxshi tushunarliyini va tashqi tizimlar bilan muvofiqligini ta'minlash uchun qo'llanishga e'tibor berish zarur.

3. Kalit tuzish va boshqarish: Shifrlash standartlari keng qo'llanildikda kalitlarni to'g'ri tuzish, saqlash va boshqarish muhimdir. Kalitlar uchun xavfsiz saqlash joylari, kalitlar va ruxsat etilgan foydalanuvchilarga ulashishning yo'llari katta e'tkazib beradi. Bu qo'llanishda amaliyot, nazorat va tajribali kadrlarning mavjudligi zarurdir.

Shifrlash standartlari, ma'lumotlarni xavfsiz tarzda almashish, himoya qilish, va maxfiylikni ta'minlashda kritik ahamiyatga ega. Ularning foydalarini va kamchiliklarini tushunish va qo'llanish sohasidagi eng so'nggi o'zgarishlarni kuzatish juda muhimdir. Xususan, shifrlash standartlari va protokollari o'zgartirilishlarga va yanada xavfsizlikni ta'minlashga qodir bo'lishi kerak, chunki yoritish tuzatish bilan birga xattacklar va boshqa xavfsizlik tahlillari ham yanada kuchayadi.

Shifrlash standartlari va protokollari faqatgina o'zgarishlarni talab qilish, balki turli sohalardagi yangiliklarga va ommaviy maqsadlarga mos kelish kerak. Masalan, IoT (Internet of Things) hamda mobil va bulut xizmatlari kabi yangi texnologiyalar shifrlash standartlarining yangilanishini talab qiladi. O'zgaruvchan mahsulotlar va xavfsizlik uskunalari bilan birga, shifrlash standartlari ham o'zgartirilishi va yangilanishi lozim bo'lgan yo'lga kirmoqda.

Shifrlash standartlari va protokollari haqida ko'proq malumot olish, xususan shifrlash sohasidagi so'nggi yangiliklarga ega bo'lish, iste'molchilar uchun o'zlarining xavfsizlik

talablari va muammolarini tushunish uchun zarur. Standartlardagi o'zgarishlarni takomillashtirish uchun xalqaro shifrlash sohasidagi yangiliklarni kuzatish va tanlash maqbul.

Shifrlash standartlari va protokollari, hukumat tashkilotlari, axborot texnologiyalari kompaniyalari, banklar, telekommunikatsiya sohasi va boshqa sohalarda xavfsizlikni ta'minlashga qiziqishlar uchun katta ahamiyatga ega. Ularning muhimligi va o'zgarishlarga mos kelishlari bilan birga, shifrlash sohasidagi yangiliklarni kuzatish, takomillashtirish va ularga amal qilishda yo'l qo'ymoq muhimdir.

Shifrlash standartlarining afzalliklari va kamchiliklarini ko'rib chiqishdan oldin, ularning to'liq tasvirlanishi uchun quyidagi faktorlarni ta'kidlash lozim:

AFZALLIKLAR:

1. Xavfsizlik darajasining yuqori bo'lishi: Shifrlash standartlari ma'lumotlarni yuqori darajada xavfsizlik bilan almashishga imkon beradi. Ularning qabul qilingan algoritmlari va protokollari texnologik ravishda rivojlangan va katta miqdorda sinovdan o'tganligi sababli yuqori darajada xavfsizlik ta'minlashga imkon beradi.

2. Global amalga oshirilishi: Shifrlash standartlari ommaviy sifatda qo'llaniladi va ularga ko'plab sohalarda yordam beradi. Ular, banklar, telekommunikatsiya sohasi, axborot texnologiyalari kompaniyalari va hukumat tashkilotlari tomonidan dunyoda ommabop tarqatilgan va qo'llaniladigan standartlar sifatida qabul qilinadi.

3. Moslashtirish: Shifrlash standartlari turli platformalar, tizimlar va tahlilgarlar orasidagi ma'lumot almashishni osonlashtirish uchun moslashtiriladi. Bu, interoperatsiyani oshiradi va turli xavfsizlik protokollarini bir-biriga bog'lab borishni osonlashtiradi.

4. Ko'pgina variantlarni taqdim etish: Shifrlash standartlari odatda bir nechta shifrlash algoritmlarini va protokollarni taqdim etadi. Bu, foydalanuvchilarga turli imkoniyatlarni taqdim etish orqali o'zlariga mos keluvchi va xavfsizlik talablariga javob beruvchi variantni tanlash imkonini beradi.

KAMCHILIKLAR:

1. Qo'llanishdan tashqari murakkablik: Shifrlash standartlari va protokollari foydalanish uchun murakkablikni talab qilishi mumkin. Bu standartlarni to'g'ridan-to'g'ri qo'llash qiyinliklarga olib kelishi va standartni amalga oshirishda yuqori darajada mutaxassislik talab etishi mumkin.

2. Kompatibilitet muammolari: Shifrlash standartlari o'zaro kompatibilitet muammolari va protokollarni tanlash, o'rnatish va boshqarish jarayonida kamchiliklar tug'dirishi mumkin. Turli protokollar, algoritmlar va platformalar orasidagi moslashtirish va tarqatish muammolari o'zgaruvchanliklarni yaratishi mumkin.

Shifrlash standartlariga quyidagi misollar bilan ko'rish mumkin:

1. AES (Advanced Encryption Standard): AES, simmetrik shifrlash uchun bir standart hisoblanadi. Misol uchun, bir ma'lumotni AES standarti bo'yicha 256-bit kalit bilan shifrlashda, faqat kalitni bilgan vaqtida ma'lumotni de-shifrlash mumkin. AES,

ma'lumotlarbazalar, tarmoqlar, fayllarni shifrlash va hujjatlar to'plamlarini himoya qilish uchun keng qo'llaniladi.

2. RSA: RSA, asimmetrik shifrlash uchun eng mashhur standart hisoblanadi. U standart shifrlash va elektronik imzolash uchun foydalaniladi. RSA standarti ikki kalitdan iborat bo'lib, xavfsizlik uchun bir kalit xavfsiz ma'lumotni shifrlashda ishlatiladi, ikkinchi kalit esa shifrlangan ma'lumotni de-shifrlash uchun foydalaniladi. RSA, bir nechta maqsadlar uchun foydalaniladi, masalan, internet kommunikatsiyasi, autentifikatsiya, elektronik to'lov sistemalari va boshqalar.

3. TLS/SSL (Transport Layer Security/Secure Sockets Layer): TLS va SSL standartlari internet tarmog'ida ma'lumotlar himoyasini ta'minlash uchun ishlatiladi. Ular ogohlantirilgan protokollarda amalga oshiriladigan shifrlash va autentifikatsiya mekanizmalari bilan foydalaniladi. TLS va SSL, brauzerlar va veb-serverlar orasidagi xavfsiz kommunikatsiyani ta'minlashda ishlatiladi.

4. SHA (Secure Hash Algorithm): SHA standartlari, ma'lumotlar xesh qiymatlarini generatsiya qilish uchun ishlatiladi. SHA-256, SHA-384, va SHA-512 kabi standartlar ma'lumotlar xesh qiymatlarini generatsiya qilishda keng qo'llaniladi. Ularning maqsadi, ma'lumotlarni o'zgarishsizligini tekshirish, elektronik imzolar yaratish va ma'lumotlar to'g'risida xavfsizlikni ta'minlashdir.

5. PGP (Pretty Good Privacy): PGP standarti xususiy matnlarni shifrlash va elektronik pochta xavfsizligini ta'minlash uchun foydalaniladi. U asimmetrik shifrlash, xeshlash funksiyalari, elektronik imzolash va kalitli biriktirishning bir kombinatsiyasini qo'llaydi. PGP standarti, shaxsiy foydalanuvchilar, korporativ tashkilotlar va elektronik pochta provayderlari tomonidan ko’rish kerak.

6. Diffie-Hellman Key Exchange: Diffie-Hellman standarti, asimmetrik shifrlash uchun kalit almashish protokolini ta'minlaydi. U ikki tomonlu bir almashish protokolidir, qo'shimcha har qanday yomonlatma va amalga oshirishni eng qattiq hollarda ta'qiqlaydi. Diffie-Hellman protokoli, kalit almashish orqali konfidensiallikni ta'minlashda ishlatiladi, masalan, bir munosabatda kalitni amalga oshirish uchun xavfsiz kanal yaratiladi.

7. Blowfish: Blowfish, simmetrik shifrlash uchun ishlatiluvchi bir standart hisoblanadi. U to'g'ri bo'lgan so'zlar va fayllarni shifrlashda ishlatiladi. Blowfish standarti, o'ziga xos blok-shifrlash algoritmi bilan ishlaydi va ma'lumotni bloklar va kalitlar yordamida shifrlaydi.

8. Triple DES (Data Encryption Standard): Triple DES, simmetrik shifrlash uchun ishlatiluvchi bir standart hisoblanadi. U DES algoritmining 3 marta takrorlanuvchi variantidir. Triple DES standarti, DES-ni qo'llab-quvvatlash uchun yana bir saf va kuchli kalitlarni qo'llaydi.

9. ECC (Elliptic Curve Cryptography): ECC, asimmetrik shifrlash uchun ishlatiluvchi bir standart hisoblanadi. U elliptik kurb chiziqlari asosida yaratilgan va kalitlarni foydalanishni yorqinlikda qisqa uzunlikdagi kalitlarga konvertlashda ishlatiladi. ECC standarti, kalitlar va himoya miqdorini saqlab qolishda kichik bir joy talab etadi, shuning uchun resurslarini kam sarflaydi.

10. Camellia: Camellia, simmetrik shifrlash uchun ishlatiluvchi standart hisoblanadi. U AES bilan o'xshash darajada xavfsizlikni ta'minlaydi. Camellia, blok-shifrlash algoritmi bo'lib, ma'lumotni bloklar yordamida shifrlaydi.

Bu misollar, shifrlash standartlarining bir nechta turdagi amaliyotlar va protokollarda qanday qo'llanilishini ko'rsatadi. Har bir standartning o'ziga xos afzalliklari va foydalanish sohalarining mavjudligi mavjud.

XULOSA

Shifrlash standartlari, ma'lumotlar uchun xavfsizlikni ta'minlashning muhim qismlarini o'z ichiga olgan qoidalardir. Ularning asosiy maqsadi, ma'lumotlarni shifrlash, de-shifrlash, autentifikatsiya, integritetni ta'minlash va konfidensiallikni saqlashdir. Shifrlash standartlari, turli sohalar uchun turli usullarda yaratilgan bo'lib, ularga ko'plab xususiyatlarni taqdim etadi.

SHIFRLASH STANDARTLARINING MUHIM XUSUSIYATLARI QUYIDAGILAR:

1. Xavfsizlik: Shifrlash standartlari ma'lumotlarni shifrlash orqali xavfsiz tarzda almashishga imkon beradi. Ular, foydalanuvchilar uchun faqatgina kalitni biluvchi tomonidan ma'lumotlarni de-shifrlash imkonini beradi.

2. Integritet: Shifrlash standartlari ma'lumotlarning o'zgartirilganligini aniqlash, integritetni ta'minlash va ma'lumotlar ustida tahrirlanishlar haqida ogohlantirish berish imkonini beradi. Bu, ma'lumotlarni yolg'on tahrirlar va o'zgarishlardan himoya qiladi.

3. Konfidensiallik: Standartlar ma'lumotlarni maxfiylikni ta'minlashda muhim rol o'ynayadi. Shifrlangan ma'lumotlar, faqatgina kalitni biluvchi tarafdan o'qilishi mumkin bo'ladi.

4. Autentifikatsiya: Shifrlash standartlari foydalanuvchilar tomonidan autentifikatsiya qilish, yani identifikatsiya va tasdiqlash jarayonlarini ta'minlash imkonini beradi. Bu, ma'lumotlar uchun moslashtirilgan autentifikatsiya protokollarini o'z ichiga oladi.

5. Interoperatsiya: Shifrlash standartlari o'zgaruvchan sohalar uchun mos kelishga yo'l qo'yiladi, ya'ni turli platformalar, tizimlar va tahlilgarlar orasida ma'lumot almashishni osonlashtiradi.

Shifrlash standartlarining qo'llanilishining kamchiliklari quyidagilar bo'lishi mumkin:

1. Murakkablik: Shifrlash standartlari va ularning protokollari murakkablikni talab qiladi. Ularning to'g'ridan-to'g'ri qo'llanishi va so'nggi standart versiyalariga mos kelish uchun mutaxassislik va tajriba talab etishi mumkin.

2. Kompatibilitet: Shifrlash standartlari va protokollari o'zaro kompatibilitet muammolari tug'dirishi mumkin.

FOYDALANILAGAN ADABIYOTLAR:

1. «Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

2.«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

3.«Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

4.С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

5.S.S.Qosimov. Axborot texnologiyalari. 0‘quv qoMlanma. - T.: «Aloqachi», 2006.

6.S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.