XORIJIY DAVLATLARNING ELEKTRON RAQAMLI IMZO ALGORITMLARI TAHLILI

Shermuxammedov Jasurbek Abobakir o'g'li
O'zbekiston Respublikasi Madaniyat vazirligi
Raqamlashtirish va axborot xavfsizligi bo'limi boshlig'i
Odilov Ilhom Isoq o'g'li
O'zbekiston Respublikasi Madaniyat vazirligi
Raqamlashtirish va axborot xavfsizligi bo'limi bosh mutaxassisi

Annotatsiya: *Ushbu maqolada kriptografiyaning muhim vazifalaridan biri elektron raqamli imzoga bag'ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o''rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta''minlovchi oddiy imzoning analogidir. Ushbu ishda RSA, ElGamal va DSA algoritmlarining afzalliklari va kamchiliklari qarab chiqilgan.*

Kalit so'zlar: *shifrlash algoritmlari, elektron raqamli imzo, RSA, ElGamal, DSA.*

So'nggi vaqtlarda axborot texnologiyalari kundalik hayotimizga kirib, muhim hukumat loyihalaridan tortib oddiy maishiy muammolarni yechishni ham qamrab olmoqda. Yangi texnologiyalar cheksiz imkoniyatlar va kata foyda keltirishi bilan birgalikda yangi muammolarni ham paydo qilmoqda. Ulardan biri axborotni olishi mumkin bo'lmagan shaxslar qo'liga tushishidan himoyalash muammosidir.

Axborotni himoyalashning ko'plab usullari mavjud, shunday bo'lsada ularni har birini quyidagi ikki usuldan biriga keltirishimiz mumkin: axborotni raqiblardan jidmoniy himoyalash va axborotni shifrlash.

Mazkur ish kriptografiyaning muhim vazifalaridan biri - elektron raqamli imzoga bag'ishlangan. Elektron raqamli imzo (ERI) biror hujjatning muallifini bir qiymatli o'rnatish uchun zarur. ERI biror hujjat yoki shartnomaning haqiqiyligini ta'minlovchi oddiy imzoning analogidir[1]. Elektron raqamli imzo quyidagilarni amalga oshirish imkonini beradi:

- Yaxlitlik nazorati;
- Hujjatni o'zgartirishlardan (soxtalashtirish) himoyalash;
- Mualliflikni inkor etish imkoniyatini yo'q qilish;
- Hujjatning muallifligini isbotlab tasdiqlash.

ERI ning ushbu xususiyatlari uni yuridik qiymatga ega elektron hujjat aylanishini tashkil etishda qo'llaniladi.

Elektron raqamli imzo — elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo. Elektron raqamli imzo - yopiq kalitini qo‘llagan holda axborotning kriptografik o‘zgarishi natijasida olingan va imzoning shakllanish vaqtidan boshlab elektron hujjatdagi axborotda xatolik yo‘qligini aniqlovchi

hamda imzo kaliti sertifikatini imzo egasiga taalluqligini tekshiruvchi elektron hujjatning rekviziti hisoblanadi; elektron raqamli imzo - elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzo ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo; elektron raqamli imzoning yopiq kaliti - elektron raqamli imzo kalit vositalaridan foydalangan holda hosil qilingan, faqat imzo qo‘yuvchi shaxsning o‘ziga ma’lum bo‘lgan va elektron hujjatda elektron raqamli imzo yaratish uchun mo‘ljallangan belgilar ketma-ketligi; elektron raqamli imzoning ochiq kaliti - elektron raqamli imzo kalit vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzo yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzo kalit haqiqiyligini tasdiqlash uchun mo‘ljallangan belgilar ketma-ketligi; elektron raqamli imzo kalitining sertifikati - elektron raqamli imzoning ochiq kaliti elektron raqamli imzoning yopiq kalitiga mosligini tasdiqlaydigan va elektron raqamli imzo yopiq kalitining egasiga vakolatli organ tomonidan berilgan elektron yoki qog‘oz shaklidagi hujjat; elektron raqamli imzo yopiq kalitining paroli - elektron raqamli imzoning yopiq kalitidan ruxsatsiz tarzda foydalanishdan himoya qilish uchun mo‘ljallangan shartli belgilar ketma-ketligi. elektron raqamli imzoning yopiq kaliti egasi - elektron raqamli imzo kalitini yaratgan (elektron hujjatga imzo qo‘ygan) va vakolatli organ tomonidan uning nomiga elektron raqamli imzo kaliti sertifikati berilgan jismoniy shaxs. elektron raqamli imzo kalit sertifikatini boshqarish - elektron raqamli imzo kalitining sertifikati amal qilishini to‘xtatib turish yoki qayta tiklash yoxud uni bekor qilish elektron raqamli imzo kalit sertifikatining amal qilish muddati - elektron raqamli imzo kaliti ro‘yxatga olingan vaqtdan boshlab 24 oydan oshmasligi kerak. elektron raqamli imzo kaliti sertifikatini https://e-imzo.uz internet manzilidagi shaxsiy kabinet orqali elektron raqamli imzo kaliti sertifikatining amal qilish muddati tugagunga qadar uzaytirib olish mumkin.

Raqamli imzo - bu xabar, dasturiy ta'minot yoki raqamli hujjatning haqiqiyligi va yaxlitligini tekshirish uchun ishlatiladigan matematik usul. Bu qo'lda yozilgan imzo yoki muhrlangan muhrning raqamli ekvivalenti, ammo u yanada o'ziga xos xavfsizlikni ta'minlaydi. Raqamli imzo raqamli aloqada buzg'unchilik va taqlid qilish muammosini hal qilish uchun mo'ljallangan.

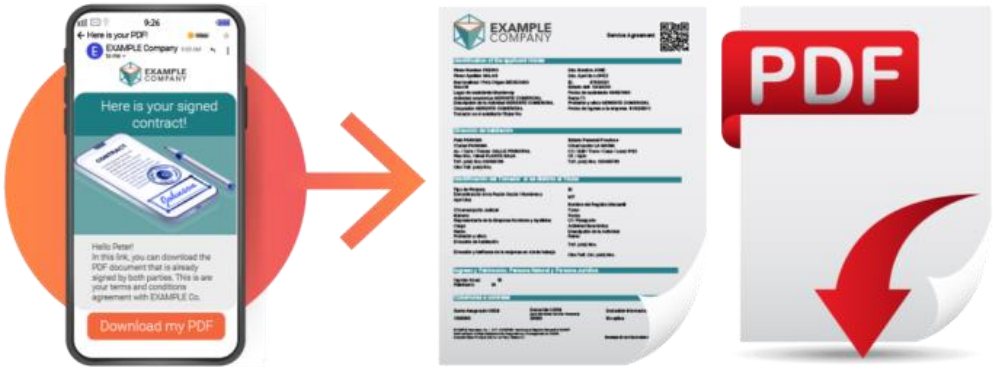
Elektron raqamli imzolar elektron hujjatlar, tranzaktsiyalar yoki raqamli xabarlarning kelib chiqishi, identifikatori va holatini tasdiqlovchi dalillarni taqdim etishi mumkin. Imzolovchilar ulardan xabardor rozilikni tasdiqlash uchun ham foydalanishlari mumkin.

Ko'pgina mamlakatlarda, jumladan, Qo'shma Shtatlarda, raqamli imzolar an'anaviy qo'lda yozilgan hujjat imzolari kabi qonuniy majburiy hisoblanadi.

Raqamli imzolar assimetrik kriptografiya deb ham ataladigan ochiq kalitli kriptografiyaga asoslangan. RSA (Rivest-Shamir-Adleman) kabi ochiq kalit algoritmidan foydalanib, ikkita kalit hosil bo'lib, matematik jihatdan bog'langan kalitlar juftligini yaratadi, biri xususiy va bitta ochiq.

Lotin Amerikasi, tartibga soluvchi heterojenlik bilan, hujjatlarni yaratish va tekshirishda raqamli va elektron imzolarning qo'llanilishi va kombinatsiyasini o'rganish

uchun noyob stsenariyni taqdim etadi. Ushbu maqola raqamli imzo va elektron imzo o'rtasidagi farqni, ularning tanlangan lotin Amerikasi mamlakatlaridagi Qonunchilik bazasini va ikkalasining kombinatsiyasi moliya sektorida hujjatli haqiqiylik uchun qanday qilib ishonchli echimni ko'rsatishi mumkinligini aniqlaydi. Maqolaning oxiriga kelib, raqamli va elektron imzoni birgalikda amalga oshirish uchun oldinga yo'l taklif etiladi, shu bilan normativ-huquqiy bazadan yoki ko'rib chiqilayotgan mamlakatdan qat'i nazar, huquqiy hujjatlarning haqiqiyligi va qaytarilmasligini kafolatlaydi.



Elektron raqamli imzo va elektron imzo: asosiy ta'riflar

Raqamli Imzo:

Hujjat yaxlitligini ta'minlash uchun assimetrik kriptografiyadan foydalaniladi.

Muassasa shaxsini tasdiqlovchi sertifikat beruvchi shaxs tomonidan berilgan raqamli sertifikatni ilova qiladi.

U yuqori darajadagi xavfsizlikni ta'minlaydi va hujjatlarni tasdiqlash uchun keng qonuniy qabul qilinadi.

Elektron imzo:

Bu qo'lda yozilgan imzoning elektron vakili.

Uning qonuniy amal qilish muddati farq qilishi mumkin va ko'p hollarda qo'shimcha shaxsni tekshirish jarayonlarini talab qiladi.

Oxirgi foydalanuvchi uchun oddiyroq va qulayroq, ammo o'zgaruvchan xavfsizlik darajasi bilan.

Raqamli sertifikat:

Raqamli sertifikat-bu jismoniy yoki yuridik shaxsni ochiq kalit bilan noyob tarzda bog'laydigan elektron hujjat. Ushbu sertifikat ishonchli sertifikatlashtirish organi tomonidan beriladi va raqamli hujjatlarning haqiqiyligi va yaxlitligini ta'minlash uchun ishlatiladi.

Sertifikatlash Sub'ektlari:

Sertifikatlashtirish sub'ektlari-bu raqamli sertifikatlar beradigan va elektron bitimda ishtirok etgan tomonlarning shaxsini tasdiqlaydigan ishonchli tashkilotlar. Ushbu sub'ektlar raqamli va elektron imzolarning xavfsizligi va haqiqiyligini ta'minlashda hal qiluvchi rol o'ynaydi.

XULOSA

DSA algoritmining kamchiligi shundan iboratki, imzolashda va imzoni tekshirishda q modul bo'yicha bo'lish amali qiyinchilik tug'diradi va maksimal tezlikda ishlash imkoniyati yo'qotiladi.

ERI algoritmlari taqqoslash

Algoritm Kalit uzunligi Imkoniyati Algoritmlar tahlili

RSA 4096 bitgacha Shifrlash va imzolash Katta sonlari faktorialini hisoblashning qiyinligiga asoslangan; dastlabki asimmetrik algoritmlardan biri. Ko'plab standartlar tarkibiga kiritilgan.

ElGamal 4096 bitgacha Shifrlash va imzolash Chekli maydonda diskret logarifmni hisoblash masalasining qiyinligiga asoslangan; bardoshlilikni kamaytirmagan holda kalitlarni qisqa vaqtda hosil qilish imkonini beradi. DSA elektron raqamli imzo algoritmining DSS standartida qo'llaniladi.

DSA 1024 bitgacha Faqat imzolash Chekli maydonda diskret logariflash masalasining qiyinligiga asoslangan; AQSh ning milliy standarti sifatida qabul qilingan; maxfiy va maxfiy bo'lmagan aloqalar uchun qo'llaniladi; AMB tomonidan ishlab chiqilgan.

FOYDALANILGAN ADABIYOTLAR:

1. Kuralov, Y. A., (2020). Development Of Geometric Creativity Of Secondary Scholl Students By Computer. International Journal of Scientific & Technology Research - (IJSTR) Volume-9 Issue-2, February 2020 Edition, 4572-4576.

2. Kuralov, Y. A., Makhmudova, D. M., (2020). METHODOLOGY OF DEVELOPING CREATIVE COMPETENCE IN STUDENTS WITH PROBLEMATIC EDUCATION. European Journal of Research and Reflection in Educational Sciences Vol. 8 No. 4, 2020, Part IIISSN 2056-5852, 142-146.

3. Akhmedov, B. A., Majidov, J. M., Narimbetova, Z. A., Kuralov, Yu. A. (2020). Active interactive and distance forms of the cluster method of learning in development of higher education. Экономика и социум, 12(79), 805-808.

4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: Радио и связь, 2001. - 376 с.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М., 2002 - 816 с.