ELEKTRON RAQAMLI IMZO

Qudratov Alijon Normamatovich,
Adilov Abduraim Nomozovich

https://doi.org/10.5281/zenodo.7313179

Annotatsiya. *Ushbu maqolada uzluksiz ta'lim tizimida zamonaviy raqamli texnologiyalarni joriy qilish tizimida electron raqamli imzo olish, elektron xujjat muallifini va xujjatning o'zini autentifikatsiyalash, ya'ni muallifning xaqiqiyligini va olingan elektron xujjatda o'zgarishlarning yo'qligini aniqlash muammosi paydo bo'ladi. Elektron xujjatlarni auentifikatsiyalashdan maqsad ularni mumkin bo'lgan jinoyatkorona xarakatlardan himoyalashdir.*

Kalit so'zlar: *Elektron xujjat, autentifikatsiya, identifikasiya, maskarad, hakkerlar, almashtirish, ochiq kalit, yo'piq kali, shifirlash, login, parolt.*

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Аннотация. *В данной статье возникает проблема получения электронной цифровой подписи, аутентификации автора электронного документа и самого документа, то есть определения подлинности автора и отсутствия изменений в полученном электронном документе, в системе внедрения современных цифровых технологий в системе непрерывного образования. Целью аутентификации электронных документов является защита их от возможной преступной деятельности.*

Ключевые слова: *электронный документ, аутентификация, идентификация, маскарад, хакеры, замена, открытый ключ, пароль, шифрование, логин, пароль.*

ELECTRONIC DIGITAL SIGNATURE

Abstract. *In this article, the problem of obtaining an electronic digital signature, authenticating the author of an electronic document and the document itself, that is, determining the authenticity of the author and the absence of changes in the received electronic document, in the system of introducing modern digital technologies in the continuous education system, appears. The purpose of authentication of electronic documents is to protect them from possible criminal activities.*

Keywords: *electronic document, authentication, identification, masquerade, hackers, replacement, Public Key, password, encryption, login, password.*

KIRISH

Elektron xujjatlarni tarmoq orqali almashishda ularni ishlash va saqlash xarajatlari kamayadi, qidirish tezlashadi. Ammo, elektron xujjat muallifini va xujjatning o'zini autentifikatsiyalash, ya'ni muallifning xaqiqiyligini va olingan elektron xujjatda o'zgarishlarning yo'qligini aniqlash muammosi paydo bo'ladi.

TADQIQOT MATERIALLARI VA METODOLOGIYASI

Elektron xujjatlarni auentifikatsiyalashdan maqsad ularni mumkin bo'lgan jinoyatkorona xarakatlardan himoyalashdir. Bunday xarakatlarga quyidagilar kiradi:

- faol ushlab qolish - tarmoqqa ulangan buzg'unchi xujjatlarni (fayllarni) ushlab qoladi va o'zgartiradi.

- maskarad – abonent *S* xujjatlarni abonent *V* ga abonent *A* nomidan yuboradi;

- renegatlik – abonent *A* abonent *V* ga xabar yuborgan bo'lsada, yubormaganman deydi;

- almashtirish – abonent *V* xujjatni o'zgartiradi, yoki yangisini shakllantiradi va uni

abonent *A* dan olganman deydi;

- takrorlash – abonent *A* abonent *V* ga yuborgan xujjatni abonent *S* takrorlaydi.

Jinoyatkorona xarakatlarning bu turlari o‘z faoliyatida kompyuter axborot texnologiyalaridan foydalanuvchi bank va tijorat strukturalariga, davlat korxona va tashkilotlariga xususiy shaxslarga ancha-muncha zarar etkazishi mumkin [1].

Elektron raqamli imzo metodologiyasi xabar yaxlitligini va xabar muallifining xaqiqiyligini tekshirish muammosini samarali hal etishga imkon beradi.

Elektron raqamli imzo telekommunikatsiya kanallari orqali uzatiluvchi matnlarni autentifikatsiyalash uchun ishlatiladi. Raqamli imzo ishlashi bo‘yicha oddiy qo‘lyozma imzoga o‘xshash bo‘lib, quyidagi afzalliklarga ega:

- imzo chekilgan matn imzo qo‘ygan shaxsga tegishli ekanligini tasdiqlaydi;
- bu shaxsga imzo chekilgan matnga bog‘liq majburiyatlaridan tonish imkoniyatini bermaydi;
- imzo chekilgan matn yaxlitligini kafolatlaydi.(1.139b).

Elektron raqamli imzo-imzo chekiluvchi matn bilan birga uzatiluvchi qo‘shimcha raqamli xabarning nisbatan katta bo‘lmagan sonidir.

TADQIQOT NATIJALARI

Elektron raqamli imzo asimmetrik shifrlarning qaytaruvchanligiga hamda xabar tarkibi, imzoning o‘zi va kalitlar juftining o‘zaro bog‘liqligiga asoslanadi. Bu elementlarning xatto birining o‘zgarishi raqamli imzoning haqiqiyligini tasdiqlashga imkon bermaydi. Elektron raqamli imzo shifrlashning asimmetrik algoritmlari va xesh–funktsiyalari yordamida amalga oshiriladi[2].

Elektron raqamli imzo tizimining qo‘llanishida bir-biriga imzo chekilgan elektron xujjatlarni jo‘natuvchi abonent tarmog‘ining mavjudligi faraz qilinadi. Har bir abonent uchun juft – mahfiy va ochiq kalit generatsiyalanadi. Mahfiy kalit abonentda sir saqlanadi va undan abonent elektron raqamli imzoni shakllantirishda foydalanadi.

Ochiq kalit boshqa barcha foydalanuvchilarga ma’lum bo‘lib, undan imzo chekilgan elektron xujjatni qabul qiluvchi elektron raqamli imzoni tekshirishda foydalanadi.

Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:

- raqamli imzoni shakllantirish muolajasi;
- raqamli imzoni tekshirish muolajasi.

Imzoni shakllantirish muolajasida xabar jo‘natuvchisining maxfiy kaliti ishlatilsa, imzoni tekshirish muolajasida jo‘natuvchining ochiq kalitidan foydalaniladi.

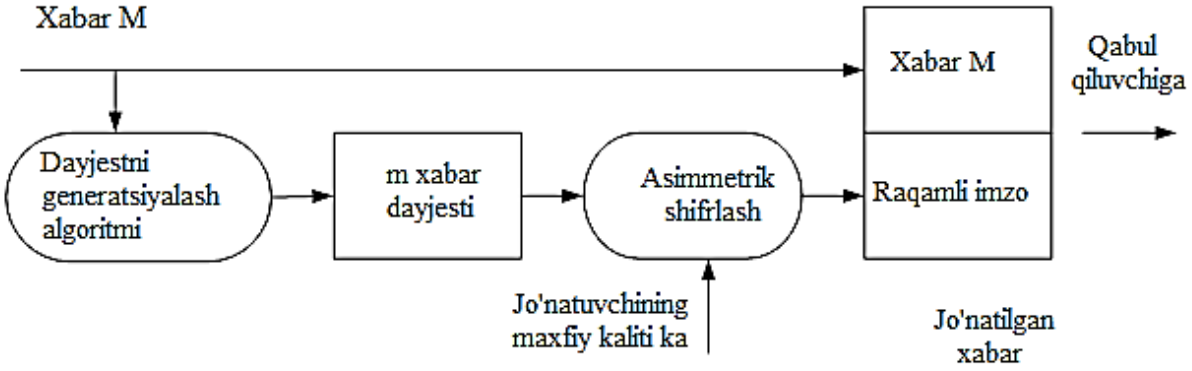
Raqamli imzoni shakllantirish muolajasi.

Ushbu muolajani tayyorlash bosqichida xabar jo‘natuvchi abonent *A* ikkita kalitni generatsiyalaydi: mahfiy kalit k_A. va ochiq kalit K_A. Ochiq kalit K_A uning jufti bo‘lgan maxfiy kaliti k_A. dan hisoblash orqali olinadi. Ochiq kalit K_A tarmoqning boshqa abonentlariga imzoni tekshirishda foydalanish uchun tarqatiladi [3].

Raqamli imzoni shakllantirish uchun jo‘natuvchi *A* avvalo imzo chekiluvchi matn *M* ning xesh funktsiyasi *L(M)*qiymatini hisoblaydi (1-rasm).

Xesh-funktsiya imzo chekiluvchi dastlabki matn *M*ni daydjest *m*ga zichlashtirishga xizmat qiladi. Daydjest *M*–butun matn *M*ni xarakterlovchi bitlarning belgilangan katta bo‘lmagan sonidan iborat nisbatan qisqa sondir. So‘ngra jo‘natuvchi *A* o‘zining mahfiy kaliti $k_A$bilan daydjest *m*ni shifrlaydi. Natijada olingan sonlar jufti berilgan *M* matn uchun raqamli

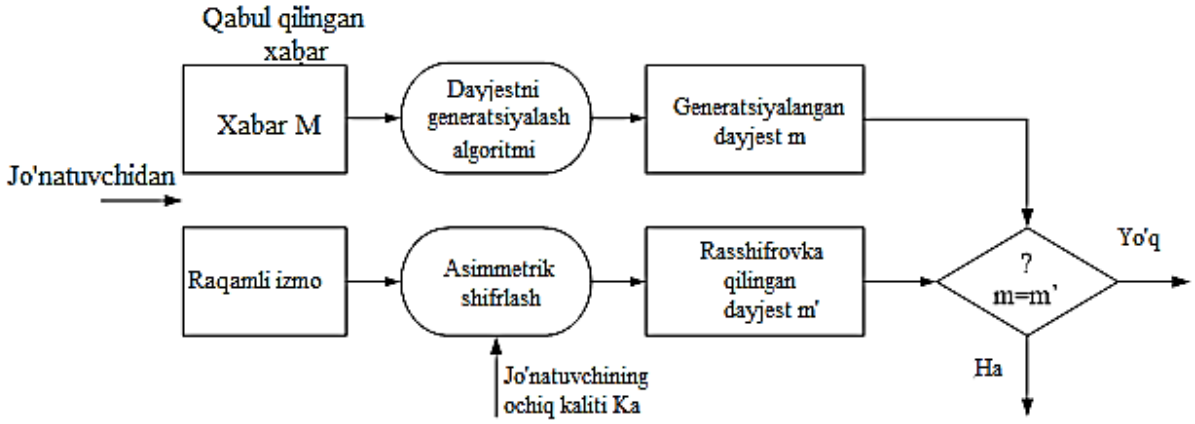
imzo hisoblanadi. Xabar *M* raqamli imzo bilan birgalikda qabul qiluvchining adresiga yuboriladi.



1-rasm. Elektron raqamli imzoni shakllantirish sxemasi.

Raqamli imzoni tekshirish muolajasi. Tarmoq abonentlari olingan xabar *M*ning raqamli imzosini ushbu xabarni jo‘natuvchining ochik kaliti K_A yordamida tekshirishlari mumkin (1-rasm).

Elektron raqamli imzoni tekshirishda xabar *M*ni qabul qiluvchi *B*qabul qilingan daydjestni jo‘natuvchining ochiq kaliti K_A yordamida rasshifrovka qiladi. Undan tashqari, qabul qiluvchini o‘zi xesh-funktsiya *h(M)* yordamida qabul qilingan xabar *M*ning daydjesti *m*ni hisoblaydi va uni rasshifrovka qilingani bilan taqqoslaydi. Agar ikkala daydjest *m* va *m’* mos kelsa raqamli imzo haqiqiy hisoblanadi. Aks holda imzo qalbakilashtirilgan, yoki axborot mazmuni o‘zgartirilgan bo‘ladi. (1.141b)



2-rasm. Elektron raqamli imzoni tekshirish sxemasi

MUHOKAMA

Elektron raqamli imzo tizimining printsipial jihati – foydalanuvchining elektron raqamli imzosini uning imzo chekishdagi maxfiy kalitini bilmasdan qalbakilashtirishning mumkin emasligidir. Shuning uchun imzo chekishdagi maxfiy kalitni ruxsatsiz foydalanishdan ximoyalash zarur. Elektron raqamli imzoning maxfiy kalitini, simmetrik shifrlash kalitiga o‘xshab, shaxsiy kalit elituvchisida, himoyalangan holda saqlash tavfsiya etiladi [4].

Elektron raqamli imzo imzo chekiluvchi xujjat va maxfiy kalit orqali aniqlanuvchi noyob sondir. Imzo chekiluvchi xujjat sifatida har qanday fayl ishlatilishi mumkin. Imzo chekilgan fayl imzo chekilmaganiga bir yoki bir nechta elektron imzo qo‘shilishi orqali yaratiladi.

Imzo chekiluvchi faylga joylashtiriluvchi elektron raqamli imzo imzo chekilgan xujjat muallifini identifikatsiyalovchi qo‘shimcha axborotga ega. Bu axborot xujjatga elektron raqamli imzo hisoblanmasidan oldin qo‘shiladi. Har bir imzo quyidagi axborotni o‘z ichiga oladi:

- imzo chekilgan sana;
- ushbu imzo kaliti ta’sirining tugashi muddati;
- faylga imzo chekuvchi shaxs xususidagi axborot (F.I.Sh., mansabi, ish joyi);
- imzo chekuvchining indentifikatori (ochiq kalit nomi);
- raqamli imzoning o‘zi.

Asimmetrik shifrlashga o‘xshash, elektron raqamli imzoni tekshirish uchun ishlatiladigan ochiq kalitning almashtirilishiga yo‘l qo‘ymaslik lozim. Faraz qilaylik, niyati buzuq odam *n* abonent *B* kompyuterida saqlanayotgan ochiq kalitlardan, xususan, abonent *A* ning ochiq kaliti $K_A$dan foydalana oladi. Unda u quyidagi xarakatlarini amalga oshirishi mumkin:

- ochiq kalit $K_A$saqlanayotgan fayldan abonent *A* xususidagi indentsifikatsiya axborotini o‘qishi;
- ichiga abonent *A* xususidagi indentifikatsiya axborotini yozgan holda shaxsiy juft kalitlari $k_n$va K_n ni generatsiyalashi;
- abonent *V*da saqlanayotgan ochiq kalit $K_A$ni o‘zining ochiq kaliti K_n bilan almashtirishi.

XULOSA

So‘ngra niyati buzuq odam *n* abonent *V* ga xujjatlarni o‘zining maxfiy kaliti k_n yordamida imzo chekib jo‘natishi mumkin. Bu xujjatlar imzosini tekshirishda abonent *V* abonent *A* imzo chekkan xujjatlarni va ularning elektron raqamli imzolarini to‘g‘ri va xech kim tomonidan modifikatsiyalanmagan deb hisoblaydi. Abonent A bilan munosabatlarini bevosita oydinlashtirilishigacha V abonentda olingan xujjatlarning xaqiqiyligiga shubha tug‘ilmaydi.

So‘rovnomani Davlat xizmatlari markazlari yoki https://e-imzo.uz sayti orqali to‘ldirish mumkin.

REFERENCES

1. G‘aniev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. T., “Aloqachi” 2008.
2. S.S.Qosimov. Axborot texnologiyalari. O‘quv qo‘llanma. — Toshkent. “Aloqachi”, 2006.
3. S.K.G‘aniev, M.M. Karimov. Hisoblash sistemalari va tarmoqlarida informatsiya himoyasi. Oliy o‘quv yur tatalabalari uchun o‘quv qo‘llanma.-Toshkent Davlat texnika universiteti, 2003.
4. Qudratov, A. N., & Yusupov, A. X. (2021). O‘QUV JARAYONIGA AXBOROT KOMMUNIKATSIYA TEXNOLOGIYALARINI QO ‘LLASH. *Science and Education*, *2*(1), 309-313.