20-Mavzu: Elektron hujjat aylanish tizimi, Davlat interaktiv xizmatlari

Reja:

20.1.Elektron hujjat tushunchasi

20.2. Elektron hujjat aylanish tizimlari

20.3. Interaktiv xizmatlar va ularda ishlash usullari

O‘zbekiston respublikasining elektron raqamli imzo bo‘yicha davlat standarti

Elektron raqamli imzoning e-biznesdagi ahamiyati, o‘zbekistonda joriy etilishi, istiqbollari va huquqiy asoslari.

elektron imzo texnalogiyasi

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. (qonun)Qonunda talab etilgan shartlarga rioya etilgan taqdirda elektron raqamli imzo qog`oz hujjatga shaxsan qo`yilgan imzo bilan bir xil ahamiyatga egadir. Elektron ma’lumotlarni kriptografik o`zgartirish natijasida hosil qilingan belgilar ketma-ketligi. Elektron raqamli imzo ma’lumotlar blokiga qo`shib qo`yiladi va blokni qabul qiluvchiga, manbani va ma’lumotlarning butunligini tekshirish hamda soxtalashtirishdan muhofazalanish imkonini beradi. Hozirgi kunga kelib, ayrim mamlakatlar qonunchilik yo`li bilan raqamli imzodan foydalanishni layoqatliligini qonunlashtirib qo`yganlar. Elektron raqamli imzo kalitlari sertifikatlari ro`yxatga olish markazlari tomonidan beriladi

Bugungi kunda butun jahonda bu borada katta ishlar amalga oshirilmoqda.Aloqa sohasida ham axborot texnologiyalari yangi pog'onaga ko'tarilmoqda.

Bu o'rinda elektron pochta, elektron hujjat alohida ahamiyatga ega. Elektron pochta o'zaro bog'langan kompyuterlar tarmog'i yordamida matbuot xabarlari (matn, rasm, chizma) va hatto tovushli axborotni foydalanuvchiga yetkazish uchun xizmat qiladi. Shuningdek, u istalgan vaqtda kerakli ma’lumotni izlash va undan foydalanish imkonini beradi.

Elektron hujjat - elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan hamda elektron hujjatning uni identifikatsiya qilish imkonini beradigan boshqa rekvizitlarga ega bo'lgan axborotdir.

Elektron hujjat quyidagi tushunchalarga asoslanadi:

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 imzoning yopiq kaliti - elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, faqat imzo qo'yuvchi shaxsning o'ziga ma’lum bo'lgan va elektron hujjatda elektron raqamli imzoni yaratish uchun mo'ljallangan belgilar ketma-ketligi;

elektron raqamli imzoning ochiq kaliti - elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzoning yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzoning haqiqiyligini tasdiqlash uchun mo'ljallangan belgilar ketma-ketligi;

elektron raqamli imzoning haqiqiyligini tasdiqlash - elektron raqamli imzoning elektron hujjatda elektron raqamli imzo yopiq kalitining egasiga tegishliligi va elektron hujjatdagi axborotda xatolik yo'qligi tekshirilgandagi ijobiy natija.

Uzoq masofadan televizion tasvirlarni qabul qilish, uzatish yoki dunyodagi barcha davlatlar bilan telefon aloqasini amalga oshirish uchun xizmat qiladigan Yer sun’iy yo'ldoshlarining ishlari ham kompyuter va maxsus dasturga asoslanganligi sir emas.

Elektron raqamli imzo va elektron raqamli imzo algoritmlarining umumiy kriptografik xossalari

Elektron raqamli imzo axborot-kommunikatsiya tarmog‘ida almashinadigan hujjatli ma’lumotlar va ularning manbalarini haqiqiy yoki haqiqiy emasligini aniqlash masalasini, ya’ni ma’lumotlar autentifikatsiyasi masalasining echimini ta’minlovchi kriptografik vosita hisoblanadi[12].

O‘zbekiston Respublikasining 2001-yilda qabul qilingan “Elektron raqamli imzo to‘g‘risida” gi qonunida berilgan ta’rif bo‘yicha 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[2].

Har qanday qog‘ozli yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo‘lgan shaxsning imzosi bo‘lishi tabiiy holdir. Imzo quyidagi ikkita maqsaddan kelib chiqib qo‘yiladi. Birinchidan, ma’lumotni olgan tomon o‘zida mavjud imzo namunasiga olingan ma’lumotdagi imzoni solishtirib, imzoning haqiqiy yoki soxtaligiga ko‘ra shu ma’lumotning haqiqiy yoki soxta ekanligini aniqlaydi. Ikkinchidan, shaxsiy imzo ma’lumot hujjatining yuridik maqomini ta’minlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir.

Qog‘ozli hujjatlarga qo‘yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab. CHunki shaxsiy imzo faqat uning muallifi tafakkurining o‘ziga xos

bo‘lgan ko‘pqirrali tomonlari mahsulidir. SHuning uchun bunday imzo muallifini hozirgi zamonaviy ilg‘or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin.

Axborot-kommunikatsiya tarmog‘ida almashinadigan elektron hujjatli ma’lumotlar ham qog‘ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo vazifasini bajaruvchi kabi elektron raqamli imzo bilan ta’minlanib, elektron hujjat va uning manbasini haqiqiy yoki haqiqiy emasligini aniqlash masalasi echimini hal etilishini talab etadi.

Elektron raqamli imzo qog‘ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo xususiyatlaridan farqli bo‘lib, ikkilik sanoq tizimi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog‘liq. Xotira bitlarining ma’lum bir ketma-ketligidan iborat bo‘lgan elektron imzoni ko‘chirib biror joyga qo‘yish yoki o‘zgartirish kompyuterlar asosidagi aloqa tizimlarida murakkablik tug‘dirmaydi[11].

1991 yilda AQSHdagi Standartlar va Texnologiyalar Milliy Instituti DSA raqamli imzo algoritmining standartini DSS yuqorida keltirilgan El Gamal va RSA algoritmlari asosida yaratib, foydalanuvchilarga taklif etgan.

ERI axborot-kommunikatsiya tarmog‘ida elektron hujjat almashinuvi jarayonida quyidagi uchta masalani echish imkonini beradi:

- elektron hujjat manbasining haqiqiyligini aniqlash;
- elektron hujjat yaxlitligini (o‘zgarmaganligini) tekshirish;
- elektron hujjatga raqamli imzo qo‘ygan sub’ektni mualliflikdan bosh tortmasligini ta’minlash.

Har qanday ERI algoritmi ikkita qismdan iborat bo‘ladi:

imzo qo‘yish;

imzoni tekshirish.

Imzo qo‘yish muallif tomonidan, faqat unga ma’lum bo‘lgan shaxsiy kalit bilan amalga oshiriladi. Imzoning haqiqiyligini tekshirish esa istalgan shaxs tomonidan, imzo muallifining ochiq kaliti bilan amalga oshirilishi mumkin.

Elektron kommunikatsiyalar va elektron hujjat almashinuvi hozirgi kunda ish yuzasidan bo‘ladigan munosabatlarning ajralmas qismi hisoblanib, har qanday zamonaviy tashkilotni elektron hujjatlar almashinuvi va Internetsiz tasavvur qilish qiyin.

Internet tarmog‘idan elektron hujjatlar almashinuvi asosida moliyaviy faoliyat olib borishda ma’lumotlar almashinuvini himoya qilish va elektron hujjatning yuridik maqomini ta’minlash birinchi darajali ahamiyat kasb etadi.

Elektron hujjatli ma’lumot almashinuvi jarayonida ERIni qo‘llash har xil turdagi to‘lov tizimlari (plastik kartochkalar), bank tizimlari va savdo sohalarining moliyaviy faoliyatini boshqarishda elektron hujjat almashinuvi tizimlarining rivojlanib borishi bilan keng tarqala boshladi.

Hozirda ERI tizimini yaratishning bir nechta yo‘nalishlari mavjud. Bu yo‘nalishlarni uchta guruhga bo‘lish mumkin:

ochiq kalitli shifrlash algoritmlariga asoslangan;

simmetrik shifrlash algoritmlariga asoslangan;

imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan raqamli imzo tizimlaridir.

Ochiq kalitli shifrlash algoritmlariga asoslangan ERI tizimlari quyidagicha tashkil qilinadi. Agar axborot-kommunikatsiya tarmog‘ining i- foydalanuvchisi j- foydalanuvchisiga imzolangan elektron hujjat jo‘natmoqchi bo‘lsa, i-foydalanuvchi o‘zining maxfiy kaliti k_i^M bilan imzolanishi kerak bo‘lgan hujjatning o‘zini shifrlab yoki uning xesh qiymatini shifrlab, shu hujjat bilan birgalikda jo‘natadi. Bu elektron hujjatni qabul qilib olgan j- foydalanuvchi, shifrlangan ma’lumotni i- foydalanuvchining ochiq kaliti k_i^o bilan deshifrlab, hosil bo‘lgan matnni hujjat matniga yoki uning xesh qiymatiga solishtiradi. Agar matnlar bilan xesh qiymatlar bir xil bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas deb qabul qilinadi.

Simmetrik shifrlash algoritmlariga asoslangan ERI tizimlari quyidagicha tashkil etiladi. i- foydalanuvchi bir vaqtning o‘zida i- foydalanuvchiga ham, j- foydalanuvchiga ham ma’lum bo‘lib, boshqa foydalanuvchilarga ma’lum bo‘lmagan k_{ij}^M- kalit bilan imzolanishi kerak bo‘lgan elektron hujjatni yoki uning xesh qiymatini shifrlab, shu hujjat bilan birgalikda jo‘natadi. Elektron hujjatni qabul qilib olgan j- foydalanuvchi, shifrlangan ma’lumotni k_{ij}^M- kalit bilan deshifrlab, hosil bo‘lgan matnni hujjat matniga yoki uning xesh qiymatiga solishtiradi. Agar matnlar bilan xesh qiymatlar bir xil bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas deb qabul qilinadi. Bunday ERI tizimi bir martalik hisoblanadi, chunki k_{ij}^M - kalitdan ikkinchi marta foydalanish imkoniyati elektron hujjatlarni soxtalashtirish imkoniyatini yaratadi. Bunday holatga chek qo‘yish uchun elektron hujjat almashinuvi ishonchli uchinchi tomon orqali amalga oshirilishi mumkin: i- foydalanuvchi o‘ziga va faqat ishonchli uchinchi tomonga ma’lum bo‘lgan kalit k_{i3}^M bilan raqamli imzoni amalga oshirib, imzolangan elektron hujjatni uchinchi ishonchli tomonga jo‘natadi, uchinchi tomon imzoning haqiqiyligini k_{i3}^M - kalit bilan tekshirib, agar haqiqiy bo‘lsa, j- foydalanuvchining o‘ziga va faqat ishonchli uchinchi tomonga ma’lum bo‘lgan kalit k_{j3}^M bilan raqamli imzoni amalga oshirib, imzolangan elektron hujjatni j- foydalanuvchiga jo‘natadi. Bunday ERI tizimi foydalanuvchilar uchun noqulay bo‘lib, ko‘plab kelishmovchiliklarni keltirib chiqaradi.

Amalda uchinchi turdagi imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan ERI tizimlaridan keng foydalaniladi.

Maxsus ERI algoritmlari raqamli imzoni hisoblash va imzoni tekshirish qismlaridan iborat. ERIni hisoblash qismi imzo qo‘yuvchining maxfiy kaliti va imzolanishi kerak bo‘lgan hujjatning xesh qiymatiga bog‘liq bo‘ladi. Imzoni tekshirish qismi imzo egasining ochiq kalitiga va qabul qilib olingan hujjatning xesh qiymatiga bog‘liq holda amalga oshiriladi.

Maxsus ERI standartlari turkumiga:

Rossiya ERI standarti: GOST R 34.10-94 va uning elliptik egri chiziqda takomillashtirilgan varianti GOST R 34.10-2001;

Amerika ERI standarti: DSA va uning elliptik egri chiziqda takomillashtirilgan varianti ECDSA -2000;

O‘zbekiston Respublikasi standarti: O‘z DSt 1092:2005; O‘z DSt 092:2009;

Germaniya standarti EC-GDSA;

Koreya standarti EC-KCDSA algoritmlari misol bo‘la oladi.[12]

Elektron raqamli imzo bitlar ketma-ketligida ifodalangan biror sondan iborat. SHuning uchun uni boshqa elektron hujjatlarga ko‘chirish yoki o‘zgartirish kiritish katta qiyinchilik tug‘dirmaydi. SHu sababli elektron hujjat almashinuvi tizimida ERIni soxtalashtirishning oldini olish chora-tadbirlari – ERI algoritmining elektron hujjatlarni soxtalashtirishga bardoshliligi masalasini echish talab etiladi.

ERI algoritmining bardoshliligi quyidagi uchta masalaning murakkabligi bilan aniqlanadi:

- imzoni soxtalashtirish, berilgan hujjatga, maxfiy kalitga ega bo‘lmagan holda to‘g‘ri imzo hisoblash;
- imzolangan ma’lumotni tashkil etish, maxfiy kalitga ega bo‘lmagan holda to‘g‘ri imzolangan ma’lumotni topish;
- ma’lumotni almashtirish, bir xil imzoga ega bo‘lgan ikkita har xil ma’lumotni topish.

Keltirilgan ERI algoritmlari standartlari bardoshliliklari diskret logarifmlash, EECHratsional nuqtalari ustida amallar bajarish va parametrli gruppa parametrini topish masalalarining murakkabligiga asoslangan.

Faktorlashtirish muammosining murakkabligiga asoslangan elektron raqamli imzo algoritmlari

RSA ochiq kalitli shifrlash algoritmi asosidagi elektron raqamli imzo

Tizimning har bir i- foydalanuvchisi (e_i, d_i)- kalitlar juftligini yaratadi. Buning uchun etarli katta bo‘lgan p va q-tub sonlari olinib (bu sonlar maxfiy tutiladi), $n = pq$-soni va Eyler funksiyasining qiymati $\varphi(n)=(p-1)(q-1)$ hisoblanadi (bu son ham maxfiy tutiladi). So‘ngra $(e_i, \varphi(n))=1$ shartni qanoatlantiruvchi, ya’ni $\varphi(n)$- soni bilan o‘zaro tub bo‘lgan e_i -son bo‘yicha d_i- soni ushbu $e_i d_i = 1 \bmod \varphi(n)$ formula orqali hisoblanadi. Bu (e_i ; d_i) –juftlikda e_i - ochiq kalit va d_i- maxfiy (shaxsiy) kalit deb e’lon qilinadi.

SHundan so‘ng i-foydalanuvchidan j-foydalanuvchiga shifrlangan ma’lumotni imzolagan holda jo‘natishi quyidagicha amalga oshiriladi:

1. SHifrlash qoidasi: $M^{e_j} \bmod n = C$, bu erda M-ochiq ma’lumot, S – shifrlangan ma’lumot;

2. Deshifrlash qoidasi: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. ERIni hisoblash: $H(M)^{d_i} \bmod n = P_i$,

bu erda i-foydalanuvchining P_i-imzosi M-ma'lumotning $H(M)$- xesh funksiya qiymati bo'yicha hisoblangan;

4. ERIni tekshirish: $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, agar $H(M) = H(M_1)$ bo'lsa (bu erda M_1 -deshifrlangan ma'lumot), u holda elektron hujjat haqiqiy, aks holda haqiqiy emas, chunki xesh funksiya xossasiga ko'ra $M = M_1$ bo'lsa, ularning xesh qiymatlari ham teng bo'ladi.

5. Ma'lumotni maxfiy uzatish protokoli:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

6. Maxfiy uzatilgan ma'lumotni qabul qilish protokoli:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, umuman qaraganda dastlabki ma'lumot

o'zgartirilgan bo'lishi mumkin, shuning uchun $C^{d_j} \bmod n = M_1 \cup P_i$ bo'lib, natijada xesh qiymat imzo bo'yicha ushbu ifoda $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ bilan hisoblanadi va qabul qilib olingan ma'lumotning xesh qiymati $H(M_1)$ bo'lsa, u holda $H(M) = H(M_1)$ bo'lganda elektron hujjat haqiqiy, aksincha bo'lsa, soxta hisoblanadi[11, 15].

ESIGN raqamli imzo algoritmi

ESIGN – YAponiya (NTT, Japan) olimlari tomonidan ishlab chiqilgan ERI algoritmidir. Bu algoritm bardoshliligi RSA algoritmi kabi faktorlashtirish muammosining murakkabligi bilan belgilanadi.

ESIGN algoritmida maxfiy kalit sifatida katta tub p va q sonlar juftligi xizmat qiladi va ular bo'yicha $n = p^2*q$ ifoda bilan aniqlanadi. Oshkora kalit bo'lib (n, k) juftligi xizmat qiladi. Bu erda k – xavfsizlik parametridir.

ESIGN algoritmi bo'yicha ERI shakllantirish va uni uzatish quyidagi qadamlar ketma-ketligini o'z ichiga oladi[21]:

1) M axborot uchun xesh-funksiya hisoblanadi:

m = H(M); m ning qiymati 0 dan n-1 oraliqda joylashgan;

2) p*q dan kichik bo'lgan tasodifiy x son generatsiyalanadi;

3) juda kichik bo'lgan butun son w hisoblanadi:

$w \equiv ((m - x^k) \pmod n)/p*q$;

4) maxfiy kalitdan foydalanib m uchun ERI S shakllantiriladi:

$S \equiv x+((w/kx^{k-1} \pmod p))p*q$;

5) axborot M va ERI S aloqa kanalidan uzatiladi.

Qabul qiluvchi tomon olingan axborot M va ERI S dan foydalanib quyidagi qadamlar ketma-ketligini amalga oshiradi:

1) M axborot uchun xesh-funksiya m = H(M) hisoblanadi:

2) oshkora kalit (n, k) dan foydalanib S uchun $S^k \pmod n$ hisoblanadi;

3) n bitlar sonining ikkilanganini 3 ga bo'lganiga teng yoki katta bo'lgan, butundan ancha kichik a soni va 2^a hisoblanadi;

4) m va $m+2^a$ bilan $s^k \pmod n$ taqqoslanadi:

m = = $s^k \pmod n$;

$m+2^a = = s^k \pmod n$.

Agar $s^k \pmod n$ m ga teng yoki undan katta bo‘lsa va $s^k \pmod n$ $m+2^a$ dan kichik bo‘lsa, ERI haqiqiy, aks holda haqiqiy emas deb topiladi. Bu algoritmda x va k bilan bog‘liq hisoblashlarni oldindan bajarib qo‘yish imkoniyati mavjudligi ERI shakllantirish jarayonini tezlashtirishga imkoniyat yaratadi.

Bu algoritmda RSA bilan bir xil o‘lchamdagi kalit va imzolardan foydalanilsa, undan ko‘ra ancha tezroq ishlaydi, xavfsizligi esa RSA bilan teng bo‘ladi. ESIGNga AQSH, Kanada, Angliya va bir qancha davlatlarda patent olingan.