19-Mavzu:Elektron hukumat boshqaruv tizimi

Reja:

19.1. Elektron xukumat tushunchasi va vazifalari.

19.2. Elektron xukumatni amalga oshirishning usullari

19.3. Elektron xukumatni joriy etish jaxon tajribasi

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

Ushbu referatda Elektron Raqamli Imzo (ERI) ga tushuncha berilib, uning qo‘llanilish sabablari ko‘rib chiqiladi. Texnologiyaning dolzarbligi, ERI ning O‘zbekistonda joriy etilishi va qo‘llanilishini, huquqiy asoslar va amaldagi olib borilayotgan tadbirlar, loyihalar bilan tanishtiradi.Oxirgi yillarda elektron tijorat jahon bo‘ylab jadal rivojlanmoqda.Tabiiyki, bu jarayon moliya-kredit tashkilotlari a’zoligida amalga oshiriladi.Savdoning bu turi ommalashib borar ekan, shuni unutmaslik kerakki, “tanga” ning orqa tomoni ham mavjud.Xorijda elektron tijorat keng rivojlangan mamlakatlarda Internet orqali sotib olinadigan tovar yoki bitimning tannarxi 300 – 400 $ bilan chegaralanadi.Buning sababi tarmoqda axborot xavfsizligi muommolari yetarlicha hal qilinmaganligi bilan tushuntiriladi.BMT ning jinoyatchilikning oldini olish va u bilan kurashish Qo‘mitasi baholashiga ko‘ra kompyuter jinoyatchiligi xalqaro muommo darajasiga ko‘tarilgan. AQSH da bu jinoiy faoliyat daromadliligi bilan qurol va narkotik savdosidan keyin uchinchi o‘rinni egallaydi. Xorijlik yetakchi mutaxassislar fikriga ko‘ra elektron tijorat jarayonining rivojlanishi asosan axborot xavfsizligi sohasidagi taraqqiyot bilan belgilanadi.Xo‘sh axborot xafsizligi deganda nima tushuniladi? Axborot xavfsizligi – axborot egasi va undan foydalanuvchining moddiy va ma’naviy zarar ko‘rishiga sabab bo‘luvchi ma’lumotning yo‘qotilishini, buzilishini, ochilish imkoniyatini yo‘q qiluvchi, tasodifiy va atayin uyushtirilgan ta’sirlarga axborotning bardoshliligidir. Axborot xavfsizligiga erishishda bazis vazifalar – axborotni konfedensialligi, to‘liqligi,

unga erkin kirish yo‘li va huquqiy ahamiyatini ta’minlashdir.Huquqiy ahamiyatga ega bo‘lgan elektron hujjat almashinuvi (EHA) bugungi kunda munozarali mavzu darajasidan real hizmat turiga aylandi.Bu hizmatga talab fond bozorida elektron savdoning rivojlanishi bilan kundan – kunga oshib bormoqda.

O‘zbekistonda internet biznes rivojlanish bosqichidagi istiqbolli, yangi tijorat faoliyatidir. Bu yo‘nalishda biz ham birinchi qadamni tashladik va bizni ham jiddiy axborot havfsizligi muommolari kutyapti. Tahlillarga ko‘ra O‘zbekistonda elektron tijoratning shiddat bilan o‘sishi ERI ning on – line operatsiyalarda rasmiy ravishda keng qo‘llanilishi bilan boshlanadi.Davlatimiz Ochiq kalitlar infratuzilmasini (Public Key Infrastructure PKI) amaliyotga tatbiq etar ekan, elektron hujjat almashinuvida kriptografik kalitlarni boshqarish masalasining yechimini topishda xalqaro tajribaga ham tayanadi.Bu infratuzilma X.509 ITU-T xalqaro standarti tafsiyalarini qoniqtiruvchi raqamli sertifikatlardan foydalanishni nazarda tutadi.Mazmun jihatdan raqamli sertifikatlar funksiyasiga ko‘ra oddiy qog‘oz hujjatda imzoni tasdiqlovchi muhrning analogidir.

Hozirda ERI Internet orqali axborot almashishning qonuniy rasmiylashtirilgan jarayoni hisoblanadi.Jumladan, 2003 yil 11 dekabrda 562-II-son Ozbekiston Respublikasi “Elektron raqamli imzo to‘g‘risida” va 2004 yil 29 aprelda 611-II-son “Elektron hujjat aylanishi to‘g‘risida” qonuni qabul qilindi. Qonundan maqsad elektron raqamli imzodan foydalanish va elektron hujjat aylanishi sohasidagi munosabatlarini tartibga solishdir. Qonunga ko‘ra elektron raqamli imzodan foydalanish sohasini davlat tomonidan tartibga solishni O‘zbekiston Respublikasi Vazirlar Mahkamasi va u vakolat bergan maxsus organ amalga oshiradi. Bularga muhim komponent sifatida bir qator normativ hujjatlar, davlat standartlari va O‘zbekiston Respublikasi Prezidenti va Vazirlar Mahkamasi qarorlari qabul qilindi.2005 yil 8 iyulda O‘zbekiston aloqa va axborotlashtirish agentligi ERI dan foydalanish sohasi bo‘yicha maxsus vakolatli organ deb e’lon qilindi va 2006 yilning 15 martida O‘zbekiston Respublikasida internet-banking, himoyalangan hujjat aylanishi, elektron tijorat rivojlanishida muhim o‘rin egallaydigan ochiq kalitli infratuzilma texnologiyalaridan foydalanuvchi ERI kalitlarini ro‘yhatdan o‘tkazuvchi markaz ochildi.

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

Yuqorida keltirilgan ERI algoritmlarining asosiy kamchiliklaridan biri, buzg‘unchi kriptotizim asosiga olingan muammoni etarlicha aniq qo‘ya olganda va uning bu muammoni hal qilishga resurslari etarlicha bo‘lganda, qabul qiluvchiga kelib tushgan raqamli imzo soxta bo‘lsa, imzolovchi shaxsda imzoning soxtaligini isbotlovchi dalillar va ma’lumotlarning yo‘qligidir. O‘zbekiston milliy ERI standartini yaratishda bu kamchiliklarni bartaraf etishga e’tibor berildi. SHu maqsadda kriptografiya sohasidagi O‘zbekiston Respublikasining dastlabki davlat standarti O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari»ni yaratish uchun matematik asos sifatida parametrli algebra qabul qilingan. Unda modul arifmetikasining yashirin yo‘llar juftiga ega bo‘lgan bir tomonlama

(parametrli) funksiyasi qo‘llaniladi, bunda hisoblashlar qiyinlik darajasi bo‘yicha darajaga ko‘tarish amallari kabi engil amalga oshiriladi, funksiyani teskarilash esa diskret logarifm muammosini echish jarayonidagidan kam bo‘lmagan hisoblash sarflari va vaqt talab qiladi. An’anaviy bir tomonlama darajaga ko‘tarish funksiyasi bitta yashirin yo‘lga ega bo‘lib, u ushbu bir tomonlama funksiyaning xususiy holidir. Unda yashirin yo‘llar sonining uchta bo‘lishi mumkinligi bardoshlilikni oshirish uchun qo‘shimcha imkoniyatlar yaratadi[5].

O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari»[5]da quyidagi parametrlardan foydalaniladi:

a) p - modul, tub son, bunda $p>2^{255}$. Bu sonning yuqori chegarasi elektron raqamli imzo algoritmi muayyan amalga oshirilganda aniqlanishi kerak;

b) q – p-1 ning faktori (tub ko‘paytuvchisi) bo‘lgan tub son, bu erda $2^{254} < q < 2^{256}$.

s) R – parametr, R<q shartni qanoatlantiruvchi natural son; R parametri foydalanuvchilarning cheklangan guruhi uchun ochiq yoki birgalikdagi maxfiy kalit bo‘lishi mumkin;

d) m = H(•) - xesh-funksiya, cheklangan uzunlikdagi M xabarni 256 bit uzunlikdagi ikkilik vektorida aks ettiradi.

ERIning har bir foydalanuvchisi quyidagi shaxsiy kalitlarga ega bo‘lishi kerak:

a) (x, u, g) – butun sonlar uchligi – ERIning yopiq kaliti;

bu erda: x, u – yopiq kalitlar, 1<x, u<q shartlarni qanoatlantiruvchi tasodifiy yoki psevdotasodifiy generatsiyalangan butun sonlar;

g – yopiq kalit, $g \equiv h^{(r-1)/q} \pmod p$ yordamida hisoblanadigan butun son;

bu erda: h<p – yopiq natural son bo‘lib, ω ning 1÷q oraliq qiymatlarida faqat ω=q bo‘lgandagina $g^{\omega} \pmod p \equiv 0$ shartni qanoatlantiradi;

b) (y, z) - butun sonlar juftligi – ERIning ochiq kaliti;

bu erda: y, z – ochiq kalitlar, $y \equiv g^{x} \pmod p$ va $z \equiv g^{u} \pmod p$ ifodalar yordamida hisoblanadi;

s) (R_1, y_1) – butun sonlar juftligi – ERIning soxtaligini aniqlash kaliti;

bu erda: R_1 – nazorat kaliti (ochiq yoki yopiq), 1÷ q-1 oraliqda tanlab olingan; agar R_1 yopiq bo‘lsa, unda R_1 imzolovchi shaxs va tekshiruvchi tomon uchun birgalikdagi maxfiy kalit bo‘lishi kerak;

y_1 - seans (ochiq) kaliti, har bir elektron raqamli imzo uchun parametr bilan darajaga oshirish natijasi kabi hisoblanadi.

Foydalanuvchilar guruhi uchun p, q tub sonlari ochiq va umumiy, R esa birgalikdagi maxfiy bo‘lishi mumkin.

Standartda imzolangan xabarni p-NEW sxemasi bo‘yicha tiklash g‘oyasi va K. SHnorrning imzo uzunligini qisqartirishga yo‘naltirilgan g‘oyasidan ham foydalanilgan.

Standartda qo‘llanilgan parametrli algebra amallari nafaqat bir tomonlama funksiyani hosil etishda, balki ERIni shakllantirish va uning haqiqiyligini tasdiqlash jarayonlarida ham keng qo‘llanilgan.

Elektron raqamli imzoni shakllantirish

1) Birinchi qism

$r \equiv m \circledR g^{\backslash -k} \pmod p$,

bu erda: m=H(M), k=H(m ® x).

2) Ikkinchi qism

$s \equiv u^{-1}*(k- r*x) \pmod q$.

3) Agar μ=1, unda

$r_1 \equiv r \circledR R_1 \pmod q$,

$x_1 \equiv (k - s*u*R_1)* r_1^{-1} \pmod q$,

$y_1 \equiv g^{\backslash x1} \pmod p$.

Bu erda μ=0 seans kalitisiz ish rejimini, μ=1 seans kaliti bilan ishlash rejimini belgilaydi.

ERIning haqiqiyligini tasdiqlash

1) ERI autentifikatsiyasi

$m \equiv z^{\backslash s} \circledR y^{\backslash r'} \circledR r \pmod p$,

bu erda: m = H(M), r' ≡ r (mod q).

2) Agar μ=1 bo‘lsa, unda ERI soxtalashtirilganligini tekshirish amalga oshiriladi;

$(z^{\backslash s} \circledR y^{\backslash r'})* R_1^{-1} \equiv (z *R_1^{-1})^{\backslash\backslash s*R1} \circledR' (y_1* R_1^{-1})^{\backslash\backslash r1} \pmod p$.

Bu erda: ® - R parametr bilan ko‘paytirish amalining belgisi;

®' - $R*R_1$ parametr bilan ko‘paytirish amalining belgisi;

$^{\backslash}$ - R parametr bilan darajaga oshirish amalining belgisi;

$^{\backslash\backslash}$ - $R*R_1$ parametr bilan darajaga oshirish amalining belgisi.

Kriptobardoshliligi daraja parametri muammosining murakkabligiga asoslangan ERI kriptotizimlarini yaratishga hamda tilga olingan umumiy sxema usulida yondashuv maqsadga muvofiqdir.

Diskret logarifmlashning murakkabligiga asoslangan sxemalarning zaif tomoni shundaki, badniyat kriptotahlilchi diskret logarifm muammosini hal qilish uchun etarli resurslarga ega bo‘lib, uni soxtalashtirgan bo‘lsa, unda soxta ERI ham haqiqiy deb qabul qilinadi. Natijada qonuniy huquqqa ega foydalanuvchi tomonlarning ERI soxtaligini isbotlash imkoniyatlari yo‘qqa chiqadi. Buning oldini olish yo‘llaridan biri oshkora kalit ifodasida parametrli funksiyadan foydalanishdir. Bunda ERI kriptotizimining bardoshliligi daraja parametri muammosining murakkabligi bilan belgilanadi.

II Amaliy qism

2.1 RSA algaritmi

Hozirgi vaqtda axborotlarni himoyalashni ta’minlashning qandaydir biror texnik usuli yoki vositasi mavjud emas, ammo ko’p xavfsizlik muammolarini yechishda kriptografiya va axborotlarni kripto o’xshash almashtirishlari ishlatiladi.

Assimmetrik kriptotizimlar haqida ma’lumotlarga ega bo’lish hamda assimmetrik shifrlash algoritmlaridan foydalanishni o’rganish

Ochiq kalitli shifrlash tizimlarida ikkita kalit ishlatiladi. Axborot ochiq kalit yordamida shifrlansa, maxfiy kalit yordamida deshifrlash qilinadi.

Ochiq kalitli tizimlarini qo'llash asosida qaytarilmas yoki bir tomonli funktsiyalardan foydalanish yotadi. Bunday funktsiyalar quyidagi xususiyatlarga ega. Ma'lumki x ma'lum bo'lsa y=f(x) funktsiyani aniqlash oson. Ammo uning ma'lum qiymati bo'yicha x ni aniqlash amaliy jixatdan mumkin emas. Kriptografiyada yashirin deb ataluvchi yo'lga ega bo'lgan bir tomonli funktsiyalar ishlatiladi. z parametrli bunday funktsiyalar quyidagi xususiyatlarga ega. Ma'lum z uchun E_z va D_z algoritmlarini aniqlash mumkin. E_z algoritmi yordamida aniqlik sohasidagi barcha x uchun f_z (x) funktsiyani osongina olish mumkin. Xuddi shu tariqa D_z algoritmi yordamida joiz qiymatlar sohasidagi barcha y uchun teskari funktsiya $x=f^{-1}(y)$ ham osongina aniqlanadi. Ayni vaqtda joiz qiymatlar sohasidagi barcha z va deyarli barcha, y uchun xatto E_z ma'lum bo'lganida ham $f^{-1}(y)$ni hisoblashlar yordamida topib bo'lmaydi. Ochiq kalit sifatida y ishlatilsa, maxfiy kalit sifatida x ishlatiladi.

Ochiq kalitni ishlatib shifrlash amalga oshirilganda o'zaro muloqatda bo'lgan sub'ektlar o'rtasida maxfiy kalitni almashish zaruriyati yo'qoladi. Bu esa o'z navbatida uzatiluvchi axborotning kriptohimoyasini soddalashtiradi.

Ochiq kalitli kriptotizimlari bir tomonli funktsiyalar ko'rinishi bo'yicha farqlash mumkin. Bularning ichida RSA, El-Gamal tizimlarini aloxida tilga olish o'rinli. Hozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini ko'rsatish mumkin. RSA nomi algoritmni yaratuvchilari familiyalarining birinchi xarfidan olingan (Rivest, Shamir va Adleman).