Kriptografiyada elliptik egri chiziqlarga asoslangan shifrlash algoritmlari

Feruza Toshboyeva To'lqin qizi
Toshkent davlat iqtisodiyot universiteti
Matematika

Annotatsiya:*Ushbu maqolada kriptografiya bo`yicha tushuncha,hamda elliptik egri chiziqlarga asoslangan shifrlash algoritimlari borasida fikr yuritilgan.*

Kalit so`zlar*: axborot, kriptografiya,elliptik, algoritim,chiziq.*

Аннотация*: В данной статье рассматриваются понятие криптографии и алгоритмы шифрования, основанные на эллиптических кривых.*

Ключевые слова: *информация, криптография, эллиптика, алгоритм, линия.*

Abstract: *This article discusses the concept of cryptography and encryption algorithms based on elliptic curves.*

Keywords: *information, cryptography, elliptic, algorithm, line.*

Axborot va telekommunikasiya texnologiyalarining jadal sur`atlar bilan rivojlanib borishi turli manbalardan tez va oson yo`l bilan axborot olish imkoniyatlarini oshirdi. Tijorat korxonalari, Davlat muassasalari va alohida shaxslar axborotni elektron shaklda yaratib saqlay boshladilar. Tarmoq orqali axborotni uzatish bir zumda yuz berishi, uni saqlash esa ixcham joy egallashi, boy ma`lumotlar bazalaridan samarali foydalanish imkoniyatlari kengaya borishi axborot miqdorining jadal sur`atlar bilan o`sishiga olib keldi.Yigirma birinchi asr axborotlashtirish asri ekaniga tobora ko`pchilik ishonch hosil qilmoqda. Bu albatta ommaviy axborot va hamma bilishi mumkin va zarur bo`lgan axborot haqida gap borganda o`ta ijobiydir. Lekin konfidensial va o`ta maxfiy axborot oqimlari uchun zamonaviy axborot-kommunikasiya texnologiyalari

qulayliklar bilan bir qatorda yangi muammolarni o`rtaga qo`ymoqda. Axborot bazalarida saqlanadigan va telekommunikasiya tizimlarida aylanayotgan axborot xavfsizligiga tahdid keskin oshdi. Keyingi vaqtda, ayniqsa, Internet paydo bo`lgandan boshlab, axborot o`g`irlash, axborot mazmunini buzib qo`yish, egasidan iznsiz o`zgartirib qo`yish, tarmoq va serverlardan beruxsat foydalanish, tarmoqqa tajovuz qilish, avval qo`lga kiritilgan uzatmalarni qayta uzatish, xizmatdan yoki axborotga daxldorlikdan bo`yin tovlash, jo`natmalarni ruxsat etilmagan yo`l orqali jo`natish hollari ko`paydi.Natijada axborot xavfsizligi muammosi O`zbekiston Respublikasi uchun ham dolzarb muammoga aylandi. Bu o`z navbatida kriptologiya fanini rivojlantirish vazifalarini dolzarb muammolar qatoriga qo`ydi, chunki hozirgi kunda bu yo`l axborot xavfsizligini ta`minlash sohasida asosiy yo`ldir.Axborotni muhofaza qilish masalalari bilan kriptologiya fani shug`ullanadi. Keyingi oxirigi yillarda kriptologiya yo`nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. O`zbekiston Respublikasi Prezidentining 2007 yil 3 aprelda qabul qilgan “O`zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to`g`risida” gi PQ-614–son qarorida hamda O`zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi “O`zbekiston Respublikasini yanada rivojlantirish bo`yicha Harakatlar strategiyasi to`g`risida” gi PF-4947-son farmoyishida beshta ustuvor yo`nalishdan biri sifatida axborotni muhofaza qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o`z vaqtida va munosib qarshilik ko`rsatish kabilar ko`zda tutilgan. Elliptik egri chiziqlarMatematikada elliptik egri chiziqlarning xossalari va funksiyalari 150 yildan ortiq vaqt davomida o`rganilgan.Ulardan kriptografiya doirasida foydalanish birinchi marta 1985 yilda Vashington universitetidan Nil Koblits va IBM da Viktor Miller tomonidan alohida taklif qilingan.Elliptik egri chiziqqa asoslangan kriptotizimlar birinchi marta mobilelektron biznesxavfsizligi provayderi Certicom tomonidan ishlab chiqilgan va keyin integral mikrosxemalar va tarmoq xavfsizligi mahsulotlarini ishlab chiqaruvchi Hifn tomonidan

litsenziyalangan.3Com, Cylink Corp., Motorola, Pitney Bowes, Siemens, TRW Inc. (Northrop Grumman tomonidan sotib olingan) va Verifone kabi sotuvchilar o`z mahsulotlarida Elliptik egri chiziqqa asoslangan kriptotizimni qo`llab-quvvatladilar.Elliptik egri chiziqlar kubik egri chiziqlarning bir turi bo`lib, uning yechimlari topologik jihatdan torusga (1-rasm) ekvivalent bo`lgan fazo mintaqasi bilan chegaralangan. Geometrik nuqtai nazardan elliptik egri chiziqElliptik egri chiziq (E)da ixtiyoriy 2 ta P va Q nuqtalar tanlanib ulardan to`g`ri chiziq(L) o`tkazilganda ushbu to`g`ri chiziq elliptik egri chiziqni biror R nuqtada kesib o`tadi va shu R nuqtaning OX o`qiga nisbatan simmetrik bo`lgan nuqtasi P va Q nuqtalarning elliptik egri chiziqda yig`indisiga teng hisoblanadi.

Axborotni kriptografik himoyalash usullari bugungi kunning dolzarb masalalaridan biri hisoblanadi. Shuning uchun bardoshli kriptografik algoritmlar ishlab chiqish, ularni amalga ishlari keng miqyosda davom etmoqda. Elliptik kriptotizimlarda axborotni himoya qilishning maxsus vositalarini ishlab chiqishning hozirgi bosqichida, asosan, elliptik egri chiziqning nuqtalari ko‘rinishida ma'lumotlarning tasviri qo‘llaniladi.

Elliptik egri chziqlar deb $y^2+a_1xy+a_3y=x^3a_2x^2+a_4x+a_6$ ko’rinishidagi Veyshtrass tenglamasi orqali aniqlanuvchi egri chiziqqa aytiladi. Ratsional nuqtalarni aniqlashning tenglamalar ko’rinishdagi birinchi usulida barcha nuqtalarni aniqlashni inkon mavjud emas va qadamlab hisoblash uzoq vaqt talab qiladi. Ratsional nuqtalarni aniqlashning va qiymatlarini hisoblagan holda aniqlash usuli esa, nisbatan aniqroq va tezkor usul hisoblanadi. Bu usul orqali elliptik egri chiziqning barcha ratsional nuqtalarini aniqlash mumkin. Xulosa qilib aytadigan bo’lsak, Ratsional nuqtalarni aniqlashning va qiymatlarini hisoblagan holda aniqlash usuli samarali va tezkor usul hisoblanadi. Elliptik egri chiziq ellips yoki oval shakl emas,lekin u ikkita o`qni kesib o`tuvchi aylanma chiziq sifatida ifodalanadi, bu nuqtaning o`rnini ko`rsatish uchun ishlatiladigan grafikdagi chiziqlar.Egri chiziq butunlay simmetrik yoki grafikning x o`qi bo`ylab aks ettirilgan.EECH asoslangan kriptotizimlar kalitlarni katta tub

sonlar mahsuloti sifatida an`anaviy hosil qilish usuli o`rniga elliptik egri tenglamaning xususiyatlari orqali yaratadi.Kriptografik nuqtai nazardan, grafik bo`ylab nuqtalarni (5) tenglama yordamida shakllantirish mumkin.Agar ishlatiladigan kalit o`lchami yetarlicha katta bo`lsa, Elliptik egri chiziqqa asoslangan kriptotizimlar juda xavfsiz deb hisoblanadi.AQSh hukumatiuzatilayotgan ma`lumotlarning sezgirlik darajasiga qarab, ichki aloqalar uchun kalit o`lchami 256 yoki 384 bit bo`lgan EECH dan foydalanishni talab qiladi.Ammo EECH ga asoslangan kriptotizimlarda RSA kabi muqobillarga nisbatan ko`proq yoki kamroq xavfsiz bo`lishi shart emas.EECH ga asoslangan Kriptotizimning asosiy afzalligi ma`lumotlarni shifrlash va shifrni ochishda olinadigan o`ziga xos samaradorlikdir. Elliptik egri chiziqqa asoslangan kriptografiya, RSA kriptografiyasiga qaraganda yuqori darajada xavfsizlik ta`minlaydi. EECH asoslangan kriptotizimida ishlatiladigan maxfiylik kalitlar, RSA kriptografiyasiga qaraganda ko`p darajada qisqa bo`lishi mumkin. Buning sababi EECH asoslangan Kriptografiga, xavfsizlik darajasini oshirish uchun katta hajmdagi kalitlarga egadir, shuningdek, kalitlar orasidagi o`zaro almashtirishlar osonlik bilan amalga oshirilishi mumkin.Elliptik egri chiziqqa asoslangan kriptografiya hozirgi kunda ko`p joyda ishlatilmoqda, masalan, banklar, telekommunikatsiya kompaniyalari, internet xizmat ko`rsatuvchilari va hokazo. Shuningdek, EECH asoslangan Kriptotizimlar, mobil qurilmalarda ishlatiladigan kriptotizimlar uchun juda qulaydir.Barcha kriptotizimlar katta ehtiyojlar talab qiladi va ularga doimiy ravishda yangilash kerak. Shuning uchun, ECC ham shuningdek, boshqa kriptotizimlar ham, o`zlarining afzalliklarini va kuchli yonlarini o`rganish, ularga qarshi potentsial xavf va tahlillarga ko`ra to`g`ri kelgan holatda foydalanish kerak.

FOYDALANILGAN ADABIYOTLAR:

1.KRIPTOGRAFIYANING MATEMATIK ASOSLARI O`quv qo`llanma D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtayeva Toshkent 2018.

2.Silverman, Joseph H. The arithmetic of elliptic curves. Graduate Texts in

Mathematics, 106. Springer-Verlag, New York, 1986. [The number theory of elliptic curves at a level suitable for advanced graduate students.]

3.Silverman, J.: Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 155, Springer-Verlag, 1994.

4.Miller, Victor. Use of elliptic curves in cryptography. Advances in cryptology CRYPTO „85 (Santa Barbara, CA,), 417–426, Lecture Notes in Comput.Sci., 218, Springer, Berlin, [One of the original articles proposing the use of elliptic curves for crypto. The other is by Neal Koblitz