ELLIPTIK EGRI CHIZIQQA ASOSLANGAN KRIPTOTIZIMLAR

Yusupova S.M., AmonovA.H., Abdullayev I.K., Avazbekov M.A
Toshkent axborot texnologiyalari unversiteti
abdujabbor.madina.1989@gmail.com

Anatatsiya: *Elliptik egri chiziqqa asoslangan Kriptotizimlar ochiq kalitli kriptografiya tizimlari kabi ikkita alohida kalitni birlashtirish uchun matematik jarayondan foydalanadi va keyin ma'lumotlarni shifrlash va shifrini ochish uchun maxfiy kalitdan foydalanadi. Ulardan biri har kimga ma'lum bo'lgan ochiq kalit, ikkinchisi esa faqat ma'lumotni jo'natuvchi va qabul qiluvchiga ma'lum bo'lgan shaxsiy kalitdir.*

Kalit so'zlar: *Elliptik egri chiziq, diskerminant, elliptik egri chiziqqa o'tkazilgan urinma, elliptik egri chiziqni kesib o'tuvchi to'g'ri chiziq.*

Reja:

V. Kirish
VI. Asosiy qism
4. Elliptik egri chiziqlar
5. Geometrik nuqtai nazardan elliptik egri chiziq
6. Arifmetik nuqtani nazardan elliptik egri chiziq
VII. Xulosa
VIII. Foydalanilgan adabiyotlar

Kirish

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.

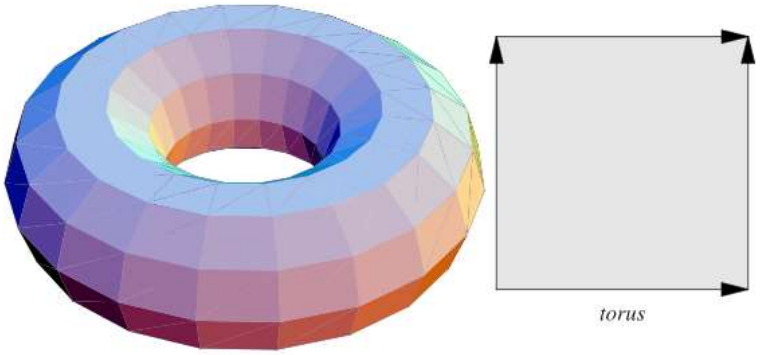
Axborotni muhofaza qilish masalalari bilan kriptologiya fani shug'ullanadi. Keyingi oxirigi yillarda kriptologiya yo'nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. O'zbekiston Respublikasi Prezidentining 2007 yil 3 aprelda qabul qilgan "O'zbekiston Respublikasida axborotning 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 chiziqlar

Matematikada 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 mobil elektron biznes xavfsizligi 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.



1-rasm. Torus

Umumiy holatda kubik egri chiziqlarning dastlabki ko'rinishi quyidagicha bo'ladi:

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0 \quad (1)$$

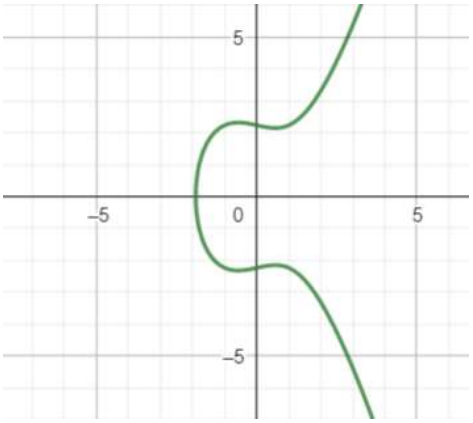
Elliptik egri chiziq esa uning xususiy ko'rinishi bo'lgani uchun uning ko'rinishi quyidagicha:

$$y^2 = x^3 + ax + b \quad (2)$$

Shuningdek, (2) tenglikning o'ng tomonini ko'paytuvchilarga ajratgan holda normal ko'rinishini yozish ham mumkin.

$$y^2 = x(x-1)(x-\lambda) \quad (3)$$

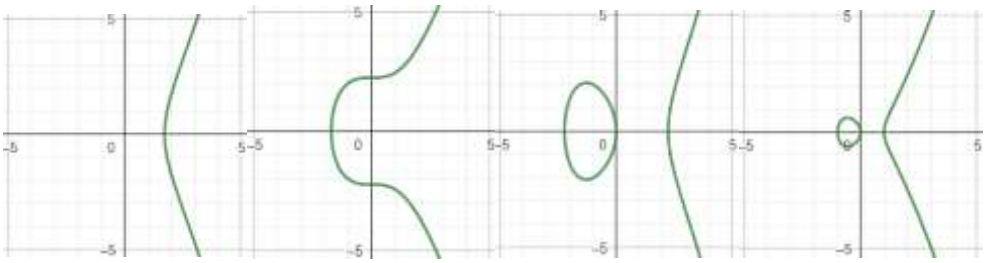
Umumiy holatda elliptik egri chiziqlarning umumiy ko'rinishi quyidagicha bo'ladi(2-rasm).



2-rasm. Elliptik egri chiziq grafigiga misol.

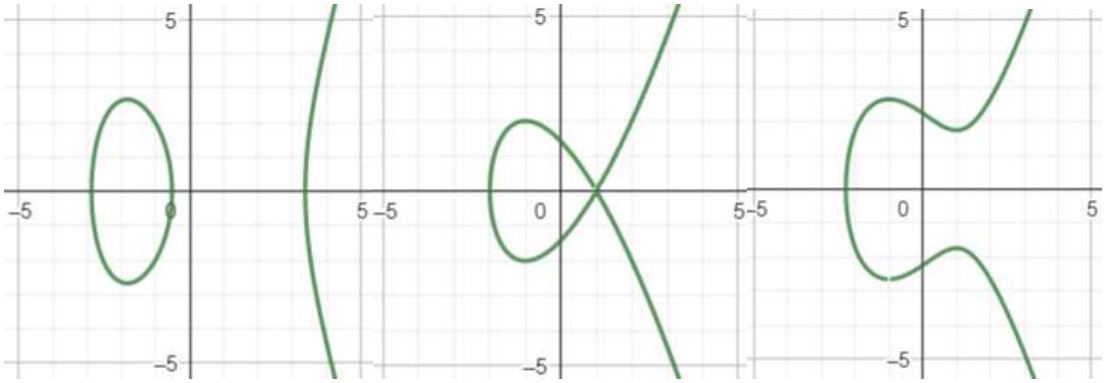
Biroq (2) formulada a=0 bo'lsa va b=0 bo'lsa grafik ko'rinishi o'zgaradi(3.1-3.2-rasmlar).

$$y^2 = x^3 - 5, \qquad y^2 = x^3 + 5, \qquad y^2 = x^3 - 5x, \qquad y^2 = x^3 - x$$



3.1-rasm. a=0. 3.2-rasm. b=0.

Grafik ko'rinishi berilgan elliptik egri chiziqning diskerminantiga bog'liq hisoblanadi(4-rasm).



$D < 0,$ $D = 0,$ $D > 0$

4-rasm. Diskerminantga bog'liq holda grafik o'zgarishi.

$$D = \Delta = 4a^3 + 27b^2 \qquad (4)$$

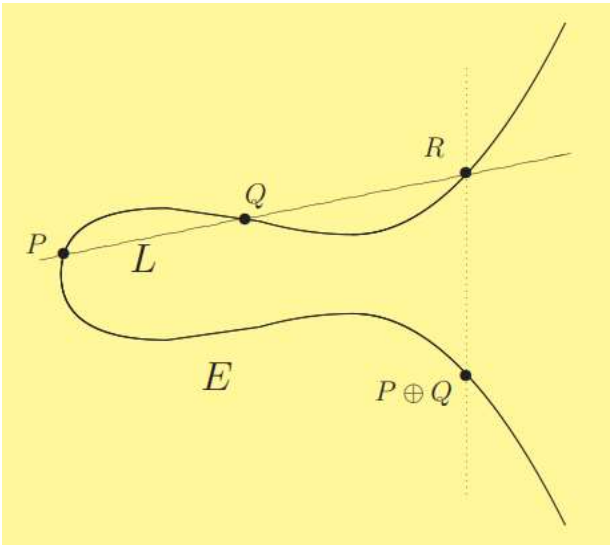
(4) – diskerminant formulasi.

Elliptik egri chiziqqa (EECH) asoslangan kriptografiya ma'lumotlarni shifrlash uchun kalitga asoslangan assimmetrik kriptotizimlar oilasiga kiruvchi muammo murakkabligiga ko'ra, Elliptik egri chiziqda diskret logorifmlash muammosining murakkabligiga asoslangan kriptotizim hisoblanadi.

(4) formuladagi diskerminant $D \neq 0$ holatlar uchun EECH asoslangan kriptotizimlarda foydalaniladi. Elliptik egri chiziqlarda nuqtalar ustida amallar bajarishda geometrik nuqtani nazardan formularga asoslanib hisob-kitob ishlari amalga oshiriladi.

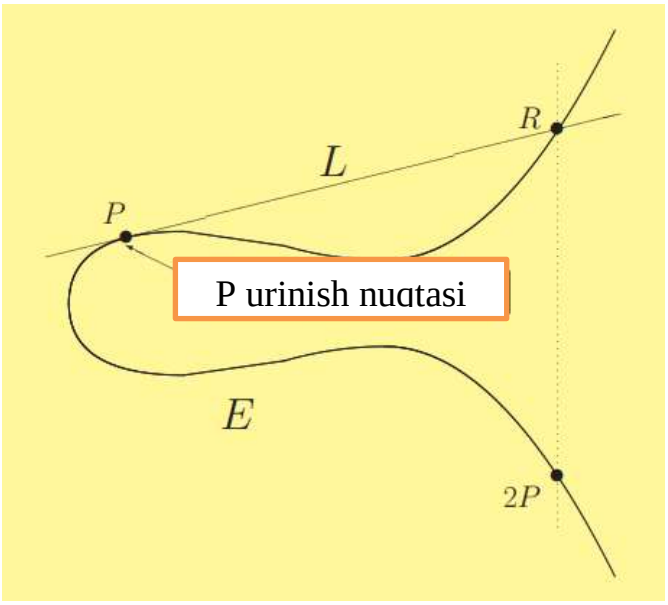
Geometrik nuqtai nazardan elliptik egri chiziq

Elliptik 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(5-rasm).



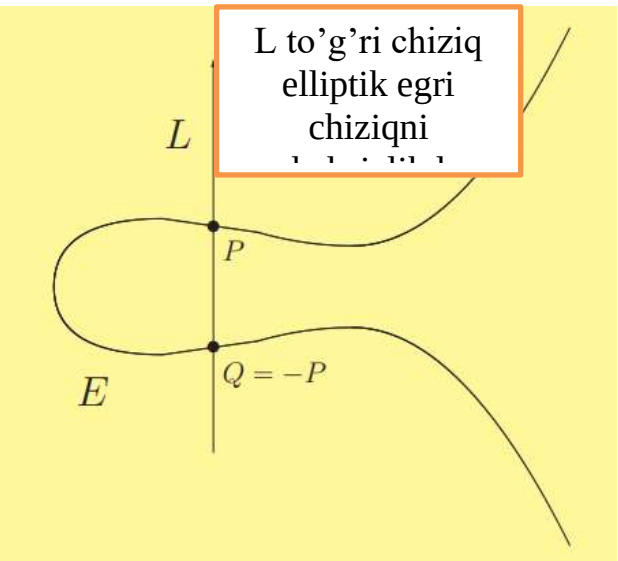
5-rasm. elliptik egri chiziqda nuqtalarning geometrik ko'rinishi.

Agar 5-rasmda (L) to'g'ri chiziq elliptik egri chiziqqa P nuqtada urinma bo'lib o'tsa ham uni R nuqtada kesib o'tadi, biroq bunda Q nuqta ham P nuqtaga teng hiosblanadi(6-rasm).



6-rasm. elliptik egri chiziqqa urinma o'tkazish.

Agarda (L) to'g'ri chiziq OY o'qiga parallel bo'lsa, unda elliptik egri chiziqni kesib o'tuvchi ikki nuqta o'zaro bir biri bilan qarama-qarshi nuqtalar bo'ladi va bunda to'g'ri chiziq elliptik egri chiziqni uchinchi nuqtada kesib o'tmaydi yoki geometrik nuqtai nazardan olib qaralganda chiksizlikda kesib o'tadi deb hisoblanadi(7-rasm).



7-rasm. To'g'ri chiziq EECH ni 2 ta qarama-qarshi nuqtalarda kesib o'tishi.

Teorema: elliptik egri chiziq (E) ustida qo'shimcha amallar

$$(a)\ P + \Theta = \Theta \quad P \epsilon E$$
$$(b)\ P + (-P) = \Theta \quad P \epsilon E$$
$$(c)\ P + (Q + R) = (P + Q) + R \quad P, Q, R \epsilon E$$
$$(d)\ P + Q = Q + P \quad P, Q \epsilon E$$

Arifmetik nuqtani nazardan elliptik egri chiziq

EECH da tanlangan ikkita nuqta $P_1 = (x_1, y_1)$ va $P_2 = (x_2, y_2)$

Elliptik egri chiziq tenglamasi $E : y^2 = x^3 + Ax + B.$ (5)

To'g'ri chiziq tenglamasi $L : y = \lambda x + \nu$ (6)

Bunda (5) va (6) tenglama orasida quyidagicha bog'lanish mavjud:

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases} \quad \text{va} \quad \text{and} \quad \nu = y_1 - \quad (7)$$

(5) va (6) tenglamalar grafikda kesishganligi tufayli ularni o'zaro tenglashtiramiz.

$$(\lambda x + \nu)^2 = x^3 + Ax + B. \quad (8)$$

(8) – formulani x_3 orqali ifodalab quyidagi natijani olish mumkin:

$$\begin{aligned} & x^3 + Ax + B - (\lambda x + \nu)^2 \\ & = (x - x_1)(x - x_2)(x - x_3) \\ & = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned} \quad (9)$$

(9) da ayniyat qoidalaridan foydalanib, soddalashtirilganda natija hosil bo'ladi:

$$-\lambda^2 = -x_1 - \quad \rightarrow \quad x_3, x_3 = \lambda^2 - x_1 - \quad \rightarrow y_3 = \lambda x_3 + \nu,$$

$$P_1 + P_2 = (x_3, -y_3).$$

Umumiy holatda quyidagi natijani olish mumkin:

$$\begin{cases} P_1 \neq P_2 \ \ va\ x_1 = x_2\ bo'lganda\ P_1 + P_2 = \Theta \\ P_1 = P_2 \ \ va\ y_1 = 0\ bo'lganda\ P_1 + P_2 = 2P = \Theta \\ \begin{cases} P_1 \neq P_2 \ \ (va\ x_1 \neq x_2) bo'lganda\ \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}\ va\ \nu = \dfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \\ P_1 = P_2 \ \ (va\ y_1 \neq 0) bo'lganda\ \lambda = \dfrac{3x_1^2 + A}{2y_1}\ va\ \nu = \dfrac{-x^3 + Ax + 2B}{2y} \end{cases} \rightarrow \\ P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2 - \nu). \end{cases}$$

Shuningdek, xususiy holatda,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \quad (10$$

$$x(2P) = \frac{x^4 - 2Ax^2 - \quad + A^2}{4(x^3 + Ax + B)} \quad (11$$

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 hukumati uzatilayotgan 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.

Xulosa

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:

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

11. 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.]

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

13. Miller, Victor. Use of elliptic curves in cryptography. Advances in cryptology CRYPTO '85 (Santa Barbara, CA, 1985), 417–426, Lecture Notes in Comput. Sci., 218, Springer, Berlin, 1986. [One of the original articles proposing the use of elliptic curves for crypto. The other is by Neal Koblitz.]

14. Koblitz, Neal. Elliptic curve cryptosystems. Mathematics of Computation 48 (1987), 203-209. [One of the original articles that proposed the use of elliptic curves for cryptography. The other is by Victor Miller.]

15. https://lib.fbtuit.uz/assets/files/4.-AkbarovD.YXasanovP.FXasanovX.PAxmedovaO.PXolimtayevaI.U.Kriptografiyaningmatematikasoslari.pdf

16. https://www.ssldragon.com/blog/what-is-openssl/#:~:text=OpenSSL%20is%20an%20all%2Daround,generation%2C%20and%20SSL%20certificate%20installation.

17. Internet sayti https://mathworld.wolfram.com/EllipticCurve.html

18. Internet sayti

https://people.math.rochester.edu/faculty/doug/otherpapers/Husemoller.pdf

19. Internet sayti:

https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf

20. https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/

21. https://xenovation.com/blog/security/pki/creating-elliptic-curve-ecdh-key-with-openssl