OPENSSL KUTUBXONASIDA ELLIPTIK EGRI CHIZIQQA ASOSLANGAN DIFFI-XELMAN ALGORITMI

Yusupova S.M., AmonovA.H., Abdullayev I.K., Avazbekov M.A
Toshkent axborot texnologiyalari unversiteti
abdujabbor.madina.1989@gmail.com1

Anatatsiya: *Elliptik egri chiziqqa asoslangan Diffi-Xelman (ECDH Elliptic Curve Diffie-Hellman) algoritmi kalit almashinuv protokolini belgilaydi. Ushbu protokol to'g'ridan-to'g'ri bir-biriga yubormasdan shifrlash uchun umumiy maxfiy kalitni yaratish uchun ishlatiladi.*

Kalit so'zlar: *elliptik egri chiziq, Diffi-Xelman algortimi, OpenSSL kutubxonasi, maxfiy kalit, ochiq kalit, kalit generatsiyalash.*

Reja:

I. Kirish
II. Asosiy qism
1. OpenSSL kutubxonasi.
2. Elliptik Egri chiziqqa asoslangan Diffi Xelman algortimi.
3. Elliptik egri chiziqqa asoslangan Diffi-Xelman algoritmi orqali OpenSSL kutubxonasida kalit generatsiyalash
III. Xulosa
IV. 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.

OpenSSL kutubxonasi

OpenSSL – bu har tomonlama kriptografiya kutubxonasi bo'lib, u TLS (Transport Layer Security – Transport qatlami xavfsizligi) protokolining ochiq manbali ilovasini taklif qiladi. Bu foydalanuvchilarga SSL (Secure Sockets Layer – ulanish qatlami xavfsizligi) bilan bog'liq turli vazifalarni, jumladan CSR (Certificate Signing Request – Sertifikat imzolash so'rovi) va shaxsiy kalitlarni yaratish va SSL sertifikatini o'rnatish imkonini beradi.

OpenSSL kutubxonadan foydalangan holda maxfiy hamda ochiq kalitlarni shuningdek, raqamli sertifikatni hosil qilish mumkin.

Elliptik Egri chiziqqa asoslangan Diffi Xelman algortimi

Elliptik egri chiziqqa asoslangan Diffi-Xelman (ECDH Elliptic Curve Diffie-Hellman) algoritmi kalit almashinuv protokolini belgilaydi. Bu yerda juda ko'p matematik amallarga yo'l qo'ymaslik uchun kalit almashinuv protokolining ketma-ketligini ko'rib chiqish:

1. domen parametrlari to'plami aloqa sheriklari o'rtasida almashinadi (sideA(A-tomon) va sideB(B-tomon))
2. sideA berilgan domen parametrlari bilan shaxsiy va ochiq kalitni yaratadi

3. sideB berilgan domen parametrlari bilan shaxsiy va ochiq kalitni ham yaratadi

4. ikkala tomon endi ochiq kalitlarini almashadilar

5. sideA endi sideB ochiq kaliti va dastlab umumiy funksiyasi bilan yangi umumiy kalitni hisoblaydi, shuningdek, olingan kalit dkB sifatida hosil bo'ladi.

6. sideB sideA ning ochiq kaliti va dastlab umumiy funksiya bilan xuddi shunday qiladi va umumiy kalitni oladi (tutilgan kalit dkA)

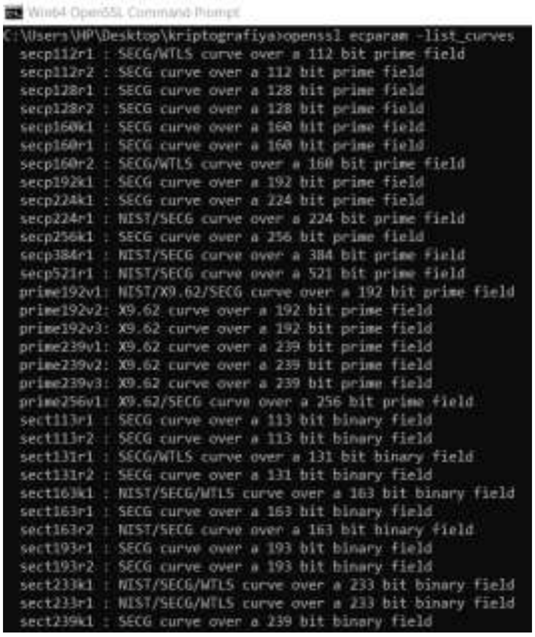
7. sideA endi xabarni deshifrlash uchun olingan dkB kalitidan foydalanishi mumkin

8. sideB, shuningdek, xabarni deshifrlash uchun olingan dkA kalitidan foydalanishi mumkin

9. Endi ikkala tomon ham o'zlarining shaxsiy kalitlari bilan xabarlarni osongina shifrlashlari va hosil qilingan dkB va dkA kalitlari bilan deshifrlashlari mumkin.

Elliptik egri chiziqqa asoslangan Diffi-Xelman algoritmi orqali OpenSSL kutubxonasida kalit generatsiyalash

OpenSSL kutubxonasiga **<openssl ecparam –list_curve>** - buyrug'ini yozib OpenSSL da mavjud Elliptik egri chiziqqa asoslangan shifrlash standartlarini ko'rish mumkin(1-rasm).

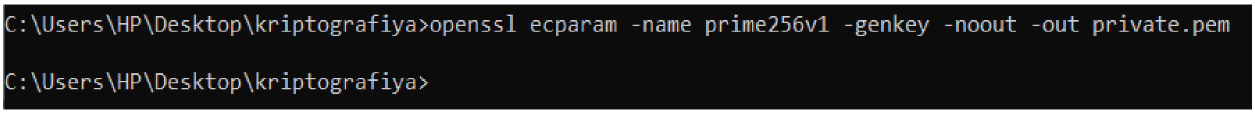


```
C:\Users\HP\Desktop\kriptografiya>openssl ecparam -list_curves
  secp112r1 : SECG/WTLS curve over a 112 bit prime field
  secp112r2 : SECG curve over a 112 bit prime field
  secp128r1 : SECG curve over a 128 bit prime field
  secp128r2 : SECG curve over a 128 bit prime field
  secp160k1 : SECG curve over a 160 bit prime field
  secp160r1 : SECG curve over a 160 bit prime field
  secp160r2 : SECG/WTLS curve over a 160 bit prime field
  secp192k1 : SECG curve over a 192 bit prime field
  secp224k1 : SECG curve over a 224 bit prime field
  secp224r1 : NIST/SECG curve over a 224 bit prime field
  secp256k1 : SECG curve over a 256 bit prime field
  secp384r1 : NIST/SECG curve over a 384 bit prime field
  secp521r1 : NIST/SECG curve over a 521 bit prime field
  prime192v1: NIST/X9.62/SECG curve over a 192 bit prime field
  prime192v2: X9.62 curve over a 192 bit prime field
  prime192v3: X9.62 curve over a 192 bit prime field
  prime239v1: X9.62 curve over a 239 bit prime field
  prime239v2: X9.62 curve over a 239 bit prime field
  prime239v3: X9.62 curve over a 239 bit prime field
  prime256v1: X9.62/SECG curve over a 256 bit prime field
  sect113r1 : SECG curve over a 113 bit binary field
  sect113r2 : SECG curve over a 113 bit binary field
  sect131r1 : SECG/WTLS curve over a 131 bit binary field
  sect131r2 : SECG curve over a 131 bit binary field
  sect163k1 : NIST/SECG/WTLS curve over a 163 bit binary field
  sect163r1 : SECG curve over a 163 bit binary field
  sect163r2 : NIST/SECG curve over a 163 bit binary field
  sect193r1 : SECG curve over a 193 bit binary field
  sect193r2 : SECG curve over a 193 bit binary field
  sect233k1 : NIST/SECG/WTLS curve over a 233 bit binary field
  sect233r1 : NIST/SECG/WTLS curve over a 233 bit binary field
  sect239k1 : SECG curve over a 239 bit binary field
```

1-rasm. OpenSSL da majvud Elliptik egri chiziq standartlari.

1-rasmdagi Elliptik egri chiziqqa asoslangan standartlarning Prime256v1 standartidan foydalanib, maxfiy kalitni hosil qilish(2-rasm).

< openssl ecparam -name prime256v1 -genkey -noout -out private.pem> - bunda private.pem maxfiy kalit elliptik egri chiziqlarning Prime256v1 standarti asosida 256 bit uzunlikdagi p maydonda hosil qilinadi.

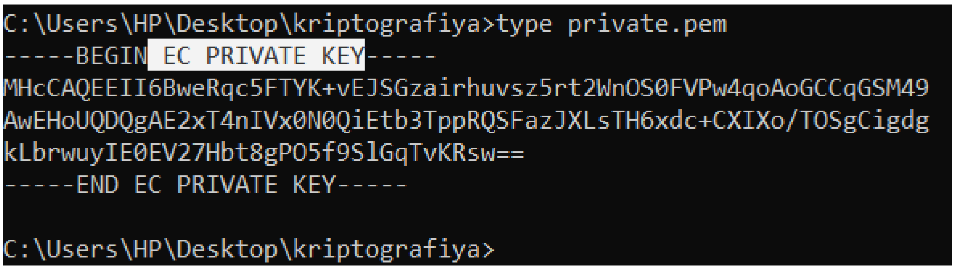


```
C:\Users\HP\Desktop\kriptografiya>openssl ecparam -name prime256v1 -genkey -noout -out private.pem

C:\Users\HP\Desktop\kriptografiya>
```

2-rasm. maxfiy kalit generatsiya qilish.

Hosil qilingan maxfiy kalitning Bloknotda ko'rinishini ko'rish uchun ***type*** buyrug'ini kirish kerak(3-rasm).



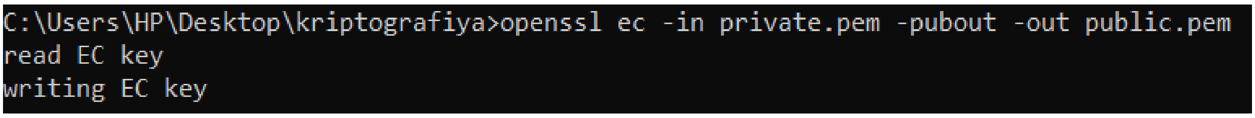
```
C:\Users\HP\Desktop\kriptografiya>type private.pem
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEII6BweRqc5FTYK+vEJSGzairhuvsz5rt2WnOS0FVPw4qoAoGCCqGSM49
AwEHoUQDQgAE2xT4nIVx0N0QiEtb3TppRQSFazJXLsTH6xdc+CXIXo/TOSgCigdg
kLbrwuyIE0EV27Hbt8gPO5f9SlGqTvKRsw==
-----END EC PRIVATE KEY-----

C:\Users\HP\Desktop\kriptografiya>
```

3-rasm. Maxfiy kalitni ko'rish.

Maxfiy kalitdan foydalangan holda ochiq(oshkor) kalit hosil qilinadi(4-rasm).

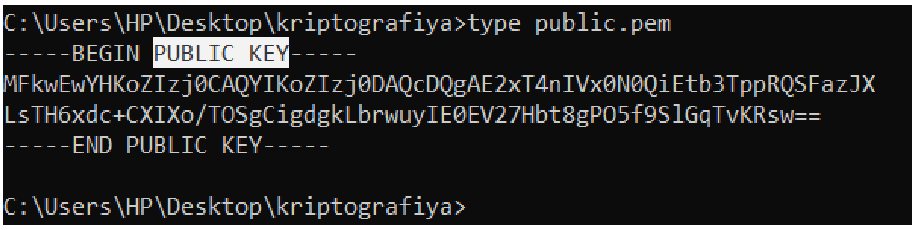
< openssl ec -in private.pem -pubout -out public.pem > -bunda Elliptik egri chiziqqa asoslanib, private.pem maxfiy kalit yordamida public.pem ochiq kalit hosil qilinadi.



```
C:\Users\HP\Desktop\kriptografiya>openssl ec -in private.pem -pubout -out public.pem
read EC key
writing EC key
```

4-rasm. maxfiy kalit yordamida ochiq kalitni hosil qilish.

Hosil qilingan ochiq kalitni ham ***type*** buyrug'ini yozish orqali Bloknotdagi ko'rinishini ko'rish mumkin(5-rasm).



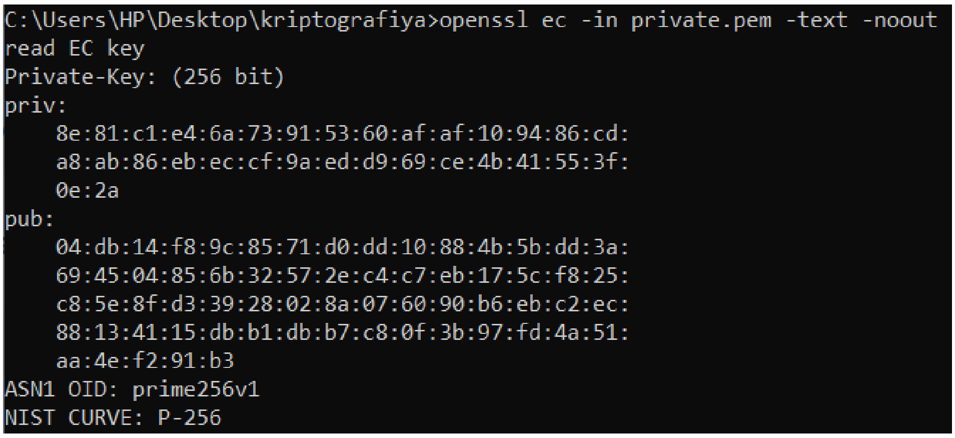
```
C:\Users\HP\Desktop\kriptografiya>type public.pem
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2xT4nIVx0N0QiEtb3TppRQSFazJX
LsTH6xdc+CXIXo/TOSgCigdgkLbrwuyIE0EV27Hbt8gPO5f9SlGqTvKRsw==
-----END PUBLIC KEY-----

C:\Users\HP\Desktop\kriptografiya>
```

5-rasm. Ochiq kalitni ko'rish.

Hosil qilingan ochiq hamda maxfiy kalitlarning o'n oltilik (0x) sanoq sistemasidagi ko'rinishini ko'rish uchun quyidagi buyruq kiritiladi(6-rasm).

< openssl ec -in private.pem -text -noout > - bunda maxfiy kalitning hamda maxfiy kalit orqali ochiq kalitning o'ng oltilik sanoq sistemasidagi ko'rinishi namoyon bo'ladi.

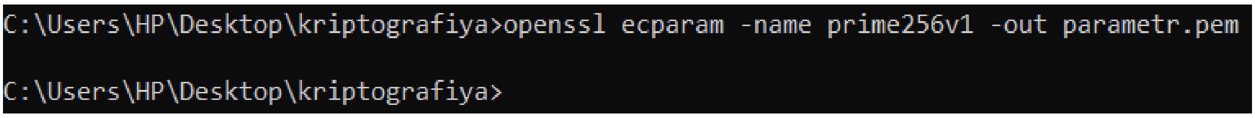


```
C:\Users\HP\Desktop\kriptografiya>openssl ec -in private.pem -text -noout
read EC key
Private-Key: (256 bit)
priv:
    8e:81:c1:e4:6a:73:91:53:60:af:af:10:94:86:cd:
    a8:ab:86:eb:ec:cf:9a:ed:d9:69:ce:4b:41:55:3f:
    0e:2a
pub:
    04:db:14:f8:9c:85:71:d0:dd:10:88:4b:5b:dd:3a:
    69:45:04:85:6b:32:57:2e:c4:c7:eb:17:5c:f8:25:
    c8:5e:8f:d3:39:28:02:8a:07:60:90:b6:eb:c2:ec:
    88:13:41:15:db:b1:db:b7:c8:0f:3b:97:fd:4a:51:
    aa:4e:f2:91:b3
ASN1 OID: prime256v1
NIST CURVE: P-256
```

6-rasm. Maxfiy hamda ochiq kalitlarning o'n oltilik sanoq tizimida ko'rinishi

Shuningdek, maxfiy kalitni parametrdan foydalangan holatda ham generatsiya qilish imkoni mavjud buning uchun qo'shimcha parametr ham generatsiya qilinishi talab etiladi(7-rasm).

< openssl ecparam -name prime256v1 -out parametr.pem > -bunda Elliptik egri chiziq asosida Prime256v1 standartidan foydalangan holda, parametr.pem nomli Elliptik egri chiziqdagi parametr hosil qilinadi.

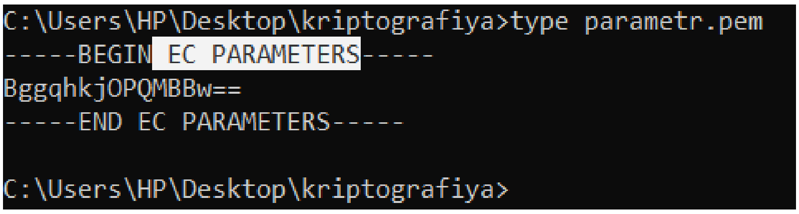


```
C:\Users\HP\Desktop\kriptografiya>openssl ecparam -name prime256v1 -out parametr.pem

C:\Users\HP\Desktop\kriptografiya>
```

7-rasm. Parametr hosil qilish.

Parametrni Bloknotdagi ko'rinishini ko'rish uchun ***type*** buyrug'ini kiritish kerak(8-rasm).



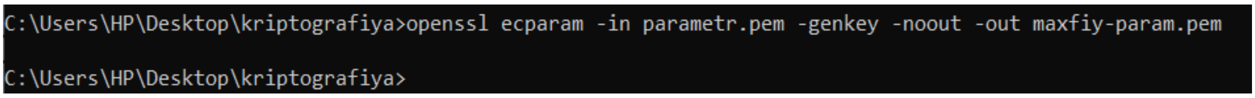
```
C:\Users\HP\Desktop\kriptografiya>type parametr.pem
-----BEGIN EC PARAMETERS-----
BggqhkjOPQMBBw==
-----END EC PARAMETERS-----

C:\Users\HP\Desktop\kriptografiya>
```

8-rasm. Parametrning ko'rinishi.

Yaratilgan parametrdan foydalangan holda maxfiy kalitni hosil qilish uchun quyidagi buyruq kiritiladi(9-rasm).

< openssl ecparam -in parametr.pem -genkey -noout -out maxfiy-param.pem> - bunda mavjud parametr.pem parametr joylashgan fayl foydalanib, maxfiy-param.pem nomdagi maxfiy kalit hosil qilinadi.

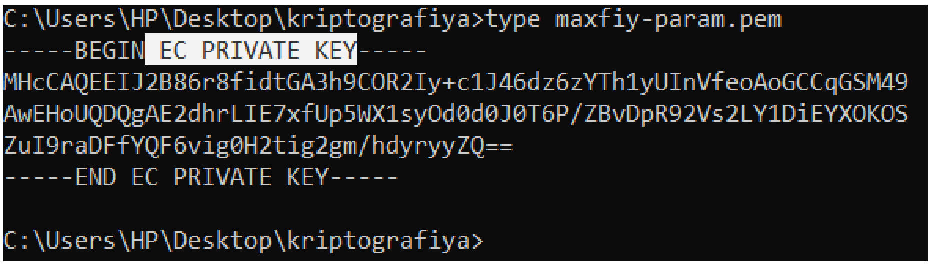


```
C:\Users\HP\Desktop\kriptografiya>openssl ecparam -in parametr.pem -genkey -noout -out maxfiy-param.pem

C:\Users\HP\Desktop\kriptografiya>
```

9-rasm. Maxfiy kalitni hosil qilish.

Hosil qilingan maxfiy kalitni ham ***type*** buyrug'ini yozish orqali ko'ris mumkin(10-rasm).

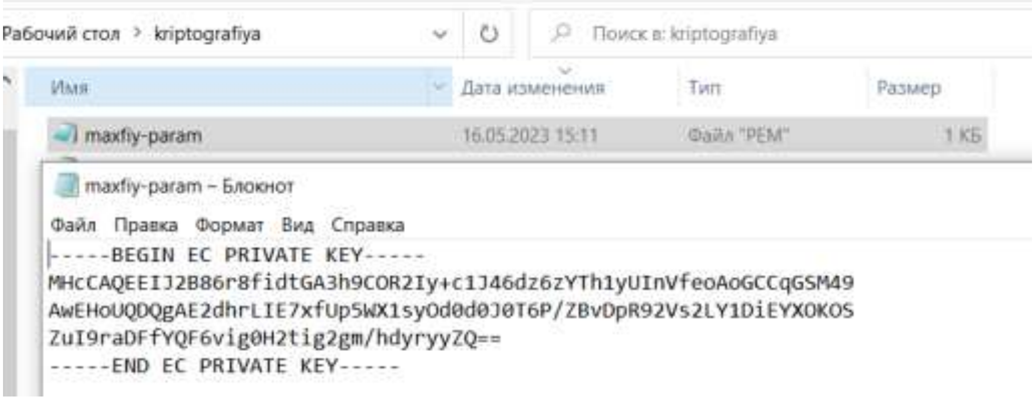


```
C:\Users\HP\Desktop\kriptografiya>type maxfiy-param.pem
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIJ2B86r8fidtGA3h9COR2Iy+c1J46dz6zYTh1yUInVfeoAoGCCqGSM49
AwEHoUQDQgAE2dhrLIE7xfUp5WX1syOd0d0J0T6P/ZBvDpR92Vs2LY1DiEYXOKOS
ZuI9raDFfYQF6vig0H2tig2gm/hdyryyZQ==
-----END EC PRIVATE KEY-----

C:\Users\HP\Desktop\kriptografiya>
```

10-rasm. Maxfiy kalitni ko'rish.

Shuningdek, maxfiy kalitni mavjud papkaga kirib ham Bloknotda ochib ko'rish mumkin(11-rasm).

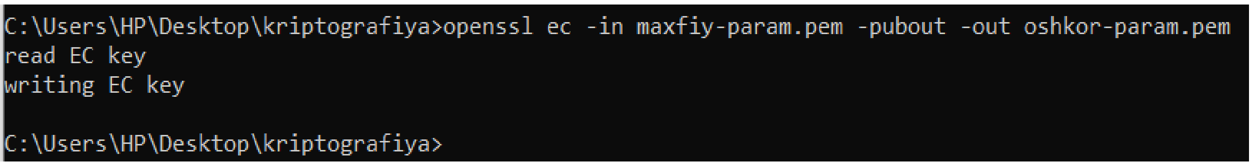


```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIJ2B86r8fidtGA3h9COR2Iy+c1J46dz6zYTh1yUInVfeoAoGCCqGSM49
AwEHoUQDQgAE2dhrLIE7xfUp5WX1syOd0d0J0T6P/ZBvDpR92Vs2LY1DiEYXOKOS
ZuI9raDFfYQF6vig0H2tig2gm/hdyryyZQ==
-----END EC PRIVATE KEY-----
```

11-rasm. Maxfiy kalitni Bloknotda ochib ko'rish.

Parameter yordamida hosil qilingan maxfiy kalit orqali ochiq kalitni hosil qilinadi(12-rasm).

e

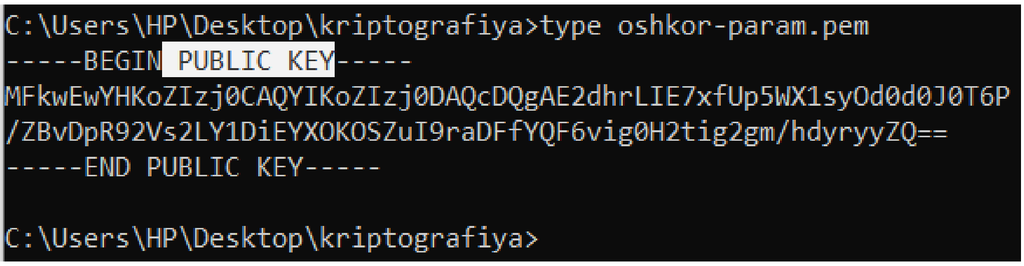


```
C:\Users\HP\Desktop\kriptografiya>openssl ec -in maxfiy-param.pem -pubout -out oshkor-param.pem
read EC key
writing EC key

C:\Users\HP\Desktop\kriptografiya>
```

12-rasm. Maxfiy kalit orqali oshkor kalitni hosil qilish.

Oshkor kalitning ko'rinishini ko'rish uchun ***type*** buyrug'ini yozish kerak(13-rasm).

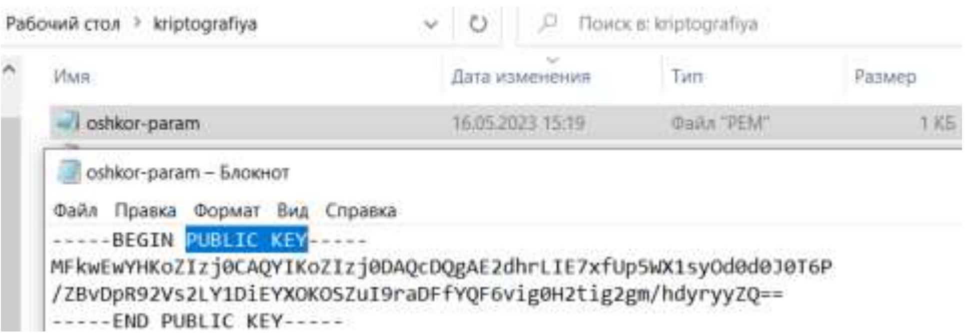


```
C:\Users\HP\Desktop\kriptografiya>type oshkor-param.pem
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2dhrLIE7xfUp5WX1syOd0d0J0T6P
/ZBvDpR92Vs2LY1DiEYXOKOSZuI9raDFfYQF6vig0H2tig2gm/hdyryyZQ==
-----END PUBLIC KEY-----

C:\Users\HP\Desktop\kriptografiya>
```

13-rasm. Oshkor kalitni ko'rish.

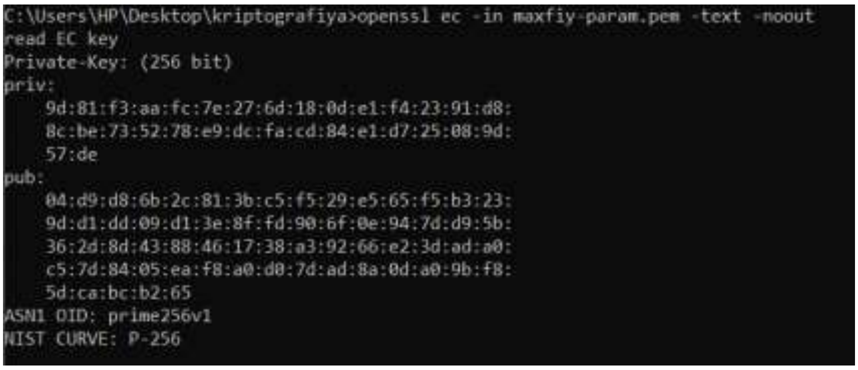
Shuningdek, oshkor kalitni ham mavjud papkaga kirib, Bloknot orqali ochib ko'rish mumkin(14-rasm).



```
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE2dhrLIE7xfUp5WX1syOd0d0J0T6P
/ZBvDpR92Vs2LY1DiEYXOKOSZuI9raDFfYQF6vig0H2tig2gm/hdyryyZQ==
-----END PUBLIC KEY-----
```

14-rasm. Oshkor kalitning bloknotdagi ko’rinishi.

Oshkor kalit hamda maxfiy kalitlarning o’n oltilik sanoq sistemasidagi jadval ko’rinishda chiqarish mumkin(15-rasm).



```
C:\Users\HP\Desktop\kriptografiya>openssl ec -in maxfiy-param.pem -text -noout
read EC key
Private-Key: (256 bit)
priv:
    9d:81:f3:aa:fc:7e:27:6d:18:0d:e1:f4:23:91:d8:
    8c:be:73:52:78:e9:dc:fa:cd:84:e1:d7:25:08:9d:
    57:de
pub:
    04:d9:d8:6b:2c:81:3b:c5:f5:29:e5:65:f5:b3:23:
    9d:d1:dd:09:d1:3e:8f:fd:90:6f:0e:94:7d:d9:5b:
    36:2d:8d:43:88:46:17:38:a3:92:66:e2:3d:ad:a0:
    c5:7d:84:05:ea:f8:a0:d0:7d:ad:8a:0d:a0:9b:f8:
    5d:ca:bc:b2:65
ASN1 OID: prime256v1
NIST CURVE: P-256
```

15-rasm. Maxfiy kalit orqali maxfiy kalit hamda oshkor kalitlarning o’ng oltilik sanoq tizimidagi jadval ko’rinish.

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:

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

1. 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.]
2. Silverman, J.: Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 155, Springer-Verlag, 1994.
3. 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.]
4. 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.]
5. https://lib.fbtuit.uz/assets/files/4.-AkbarovD.YXasanovP.FXasanovX.PAxmedovaO.PXolimtayevaI.U.Kriptografiyaningmatematikasoslari.pdf
6. https://www.ssldragon.com/blog/what-is-openssl/#:~:text=OpenSSL%20is%20an%20all%2Daround,generation%2C%20and%20SSL%20certificate%20installation.
7. Internet sayti: https://www.math.brown.edu/johsilve/Presentations/WyomingEllipticCurve.pdf
8. https://www.keyfactor.com/blog/elliptic-curve-cryptography-what-is-it-how-does-it-work/
9. https://xenovation.com/blog/security/pki/creating-elliptic-curve-ecdh-key-with-openssl