OPENSSL KUTUBXONASIDA KALIT GENERATSIYALASH USULLARI VA ALGORITMLARI

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

Anatatsiya: *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.*

Kalit so'zlar: *OpenSSL kutubxonasi, maxfiy kalit, ochiq kalit, parametr, RSA algoritmi, DSA algoritmi, DH parametri.*

Reja:

IX. Kirish
X. Asosiy qism
   7. RSA algoritmi yordamida kalit generatsiyalash.
   8. DSA algoritmi yordamida kalit generatsiyalash.
   9. DH algoritmi yordamida kalit generatsiyalash.
XI. Xulosa
XII. Foydalanilgan adabiyotlar

Kirish

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.

RSA algoritmi yordamida kalit generatsiyalash

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

1-qadam. Maxfiy ya'ni shaxsiy kalitni yarash va ko'rish (Windows da).

1) OpenSSL dasturini o'rnatib, unga kiramiz va << genrsa –aes128 –out Surayyo_private.pem 1024>> deb yozamiz (1-rasm). Bunda "genrsa –aes128" – RSA algoritmi orqali AES128 simmetrik blokli shifrlash algoritni yordamida kalit generatsiya qilinadi, kalit uzunligi 1024bit bo'lib, uni [512;4096] oraliqda tanlash mumkin. Hosil qilingan shaxsiy kalit Surayyo_private.pem fayliga joylashtiriladi (bunda fayl nomi ixtiyoriy tanlanadi)

```
OpenSSL> genrsa -aes128 -out Surayyo_private.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.+++++
.............+++++
e is 65537 (0x010001)
```

1-rasm

2) Yaratilgan shaxsiy kalitga kirish uchun *kirish paroli* o'rnatiladi va tasdiqlash uchun takrorlanadi (2-rasm).

```
e is 65537 (0x010001)
Enter pass phrase for Surayyo_private.pem:
Verifying - Enter pass phrase for Surayyo_private.pem:
OpenSSL>
```

2-rasm

3) Yaratilgan shaxsiy kalit OpenSSL dasturi joylashgan papkaga joylashadi. Uni ko'rish uchun OpenSSL joylashgan papkadan Surayyo_private nomli faylni ochib ko'rish mumkin (3-rasm).

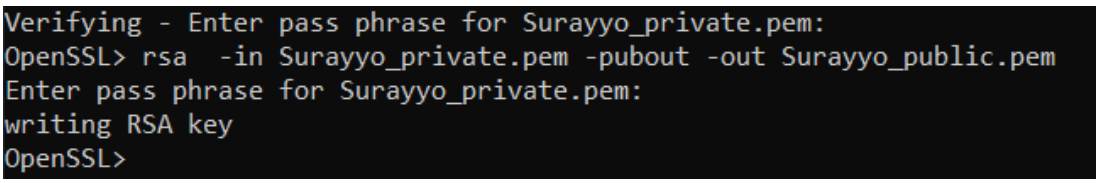
3-rasm

2-qadam. Ochiq kalitni yaratish va ko'rish (Windows da).

1) <<rsa –in Surayyo_private.pem –pubout –out Surayyo_public.pem>>

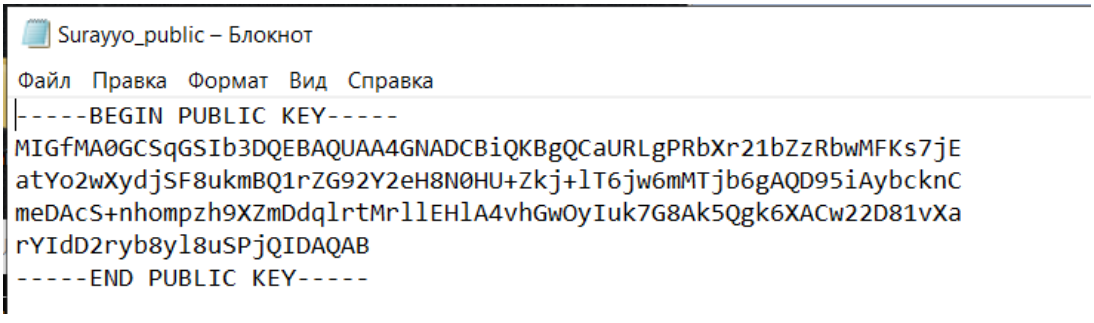
Yuqoridagi buyruq orqali ochiq kalit yaratiladi. Bunda RSA algoritmi yordamida Surayyo_private.pem (yaratilgan shaxsiy kalit)dan foydalangan holda ochiq kalit yaratiladi va Surayyo_public.pem (ixtiyoriy nomli) faylga joylashtiriladi (4-rasm).

Yuqoridagi buyruqdan so'ng shaxsiy kalitga kirish paroli so'raladi va parol to'g'ri kiritilsa, ochiq kalit yaratiladi, aks holda yaratilmaydi.



4-rasm

2) Ochiq kalitni ko'rish uchun OpenSSL joylashgan papkadan Surayyo_public nomli fayl ochib ko'riladi (5-rasm).

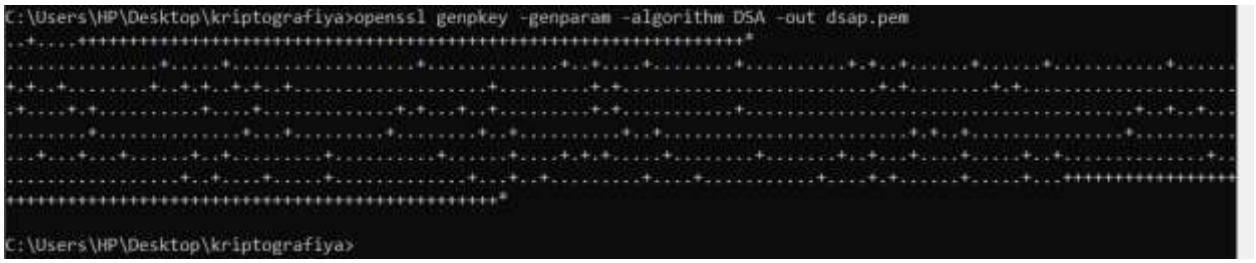


5-rasm

DSA algoritmi yordamida kalit generatsiyalash

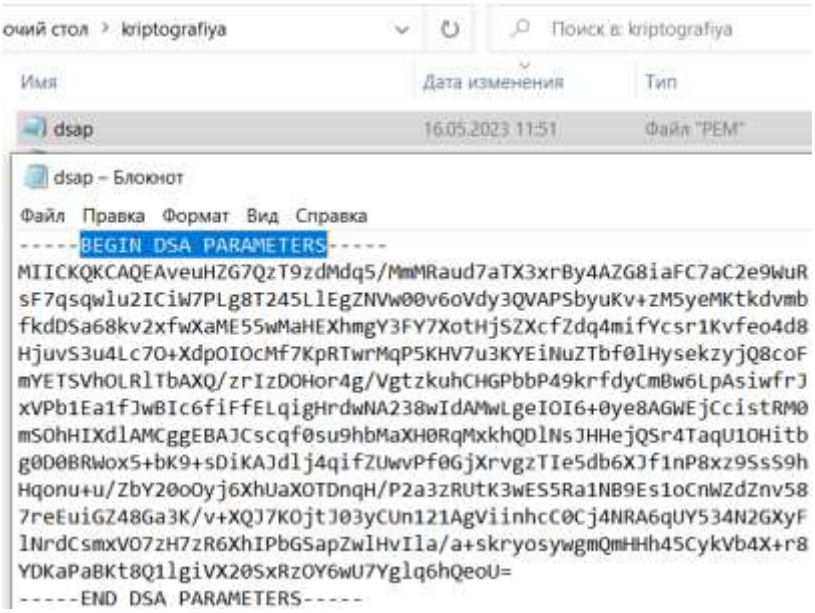
1) DSA parametrini hosil qilish(6-rasm).

<openssl genpkey –genparam –algorithm DSA –out dsap.pem> - 2048 bitli dastlabki, DSA parametrini hosil qilish, bunda dsap.pem DSA parameter saqlagan fayl nomi.



6-rasm. DSA parametrini hosil qilish.

2) yaratilgan faylni kriptografiya nomli papkaga kirib ko'rish mumkin(7-rasm).

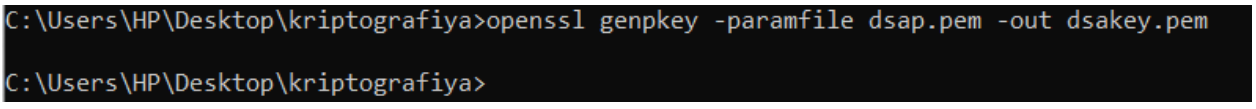


7-rasm. DSA pametrining ko'rinishi.

7-rasmdan ko'rish mumkinki, ochilgan faylning yuqori qatorida BEGIN DSA PARAMETERS – DSA parametr hosil qilingan ekanligini ko'rsatadi.

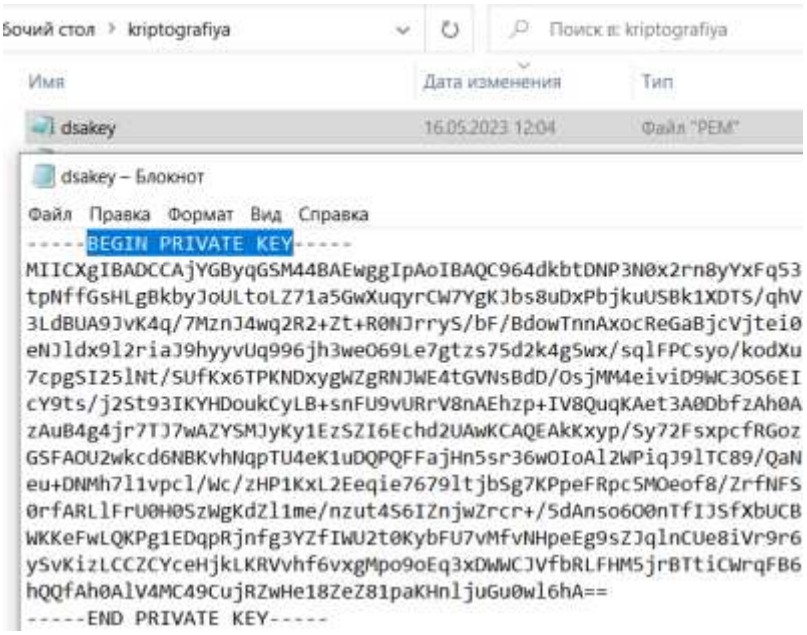
3) yaratilgan DSA parametrdan foydalanib, kalit hosil qilish(8-rasm).

<openssl genpkey -paramfile dsap.pem -out dsakey.pem> - dsap.pem nomli parameter fayldan foydalanib, kalit generatsiya qilish hamda hosil qilingan kalitni dsakey.pem faylga joylashtish.



8-rasm. DSA parametrdan foydalanib, kalit hosil qilish.

4) hosil qilingan kalitni ham kriptografiya nomli faylga kirib, topish mumkin(9-rasm).

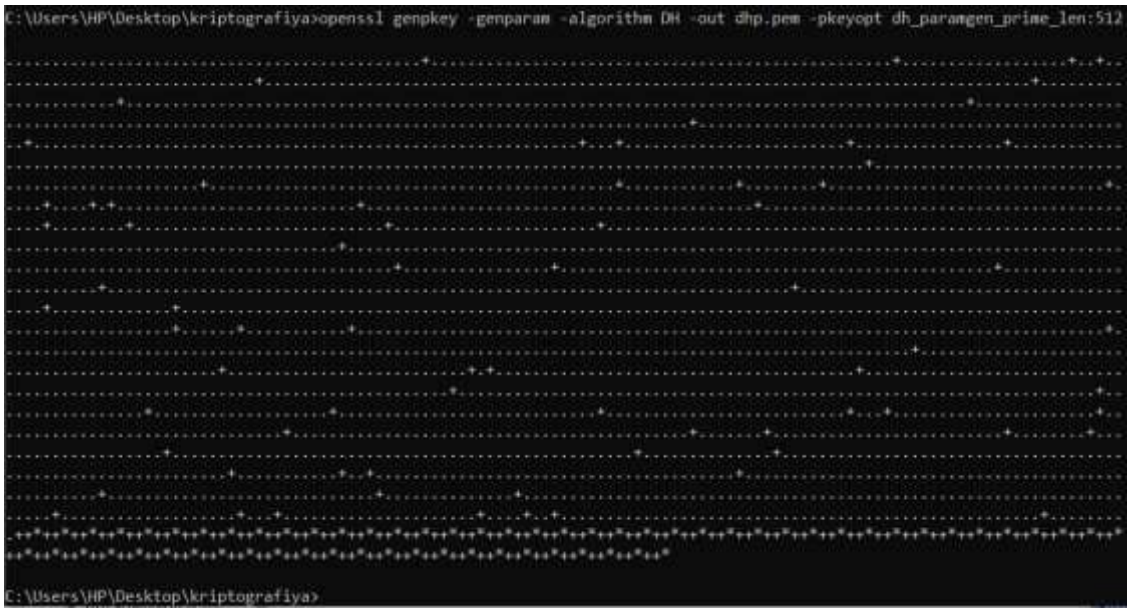


9-rasm. DSA parametrdan foydalanib, maxfiy kalit hosil qilish.

DH algoritmi yordamida kalit generatsiyalash

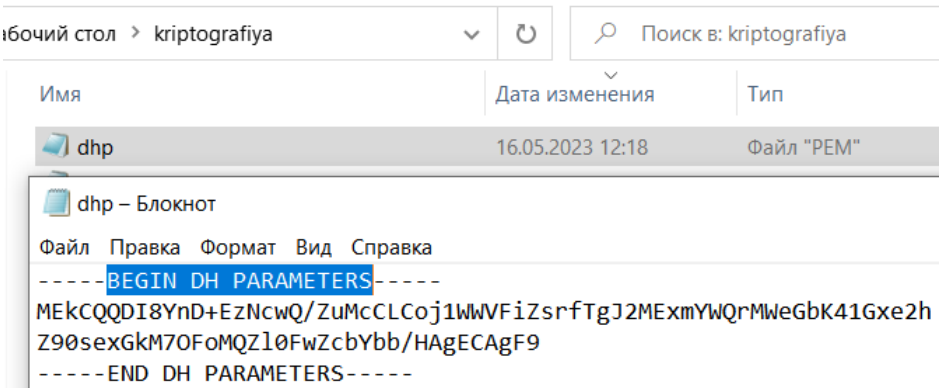
1) DH parametrini generatsiya qilish(10-rasm).

<openssl genpkey -genparam -algorithm DH -out dhp.pem -pkeyopt dh_paramgen_prime_len:512> - DH algoritmi asosida 512 bitli dhp.pem DH parametnini hosil qilish.



10-rasm. DH parametri

2) yaratilgan parametrni ochib ko'rish(11-rasm).



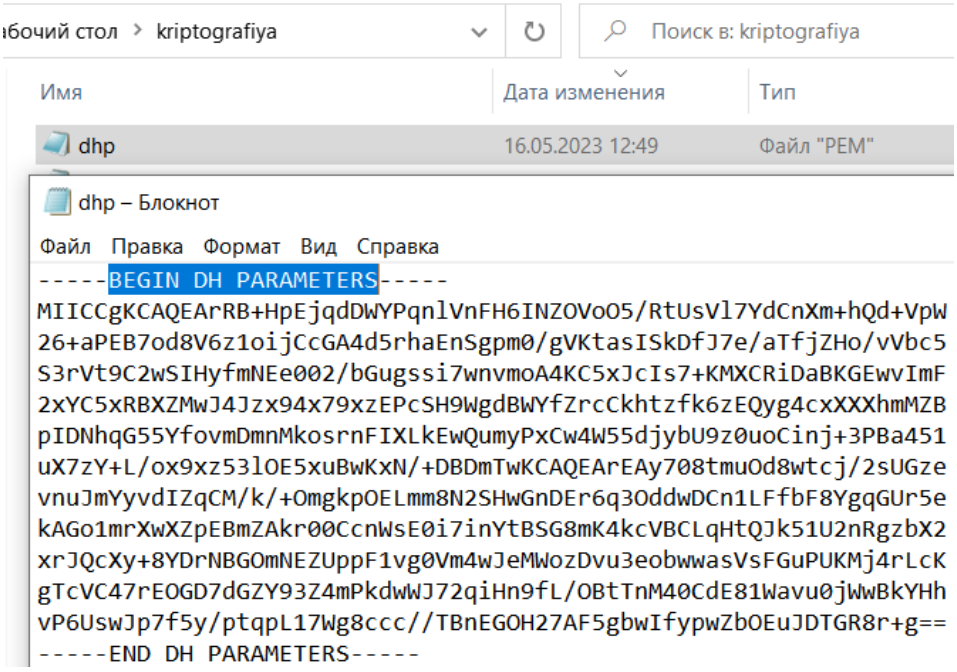
11-rasm. DH parametrining ko'rinishi.

3) DH algoritmining RFC5114 standartidan foydalanib ham DH paramertini hosil qilish(12-rasm).

<openssl genpkey -genparam -algorithm DH -out dhp.pem -pkeyopt dh_rfc5114:2> - DH algoritmnining RFC5114 standartidan foydalangan holda 2048 bitli DH paramatrini hosil qilish.

12-rasm. DH algoritmi yordamida RFC5114 standarti orqali DH parametr hosil qilish.

4) 17-rasmda hosil qilingan DH parametrni OpenSSL joylashgan papkaga kirib ko'rish mumkin(13-rasm).



13-rasm. DH parametrning ko'rinishi.

5) yaratilgan ixtiyoriy DH parametrdan foydalanib, maxfiy kalit hosil qilish(14-rasm).

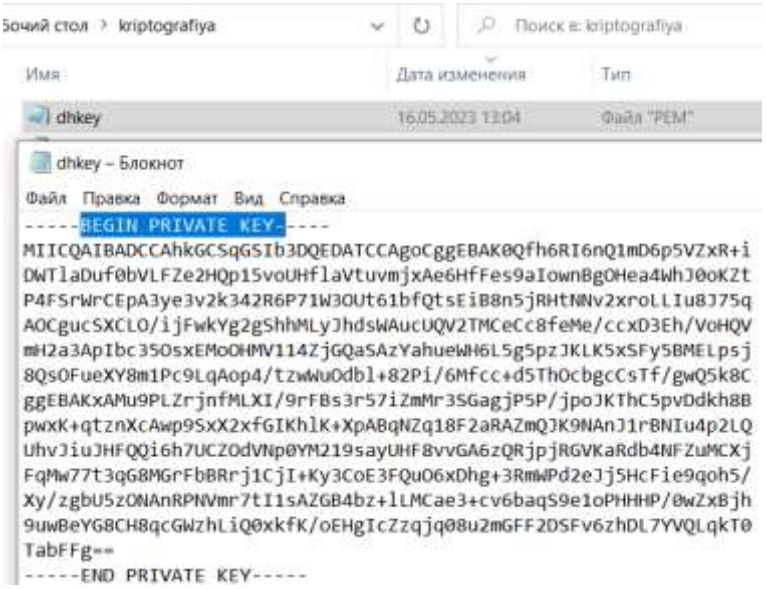
<openssl genpkey -paramfile dhp.pem -out dhkey.pem> - dhp.pem DH parametni joylashgan fayldan foydalanib, dhkey.pem mavfiy kalit hosil qilish.

```
C:\Users\HP\Desktop\kriptografiya>openssl genpkey -paramfile dhp.pem -out dhkey.pem

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

14-rasm. DH parametrdan foydalanib, maxfiy kalit hosil qilish.

6) hosil qilingan ochiq kalitni ko'rish(15-rasm).



15-rasm. Maxfiy kalit ko'rinishi.

Elliptik Egri chiziqqa asoslanib kalit generatsiyalash

1) elliptik egri chiziqqa asosida kalit genratsiyalash(16-rasm).

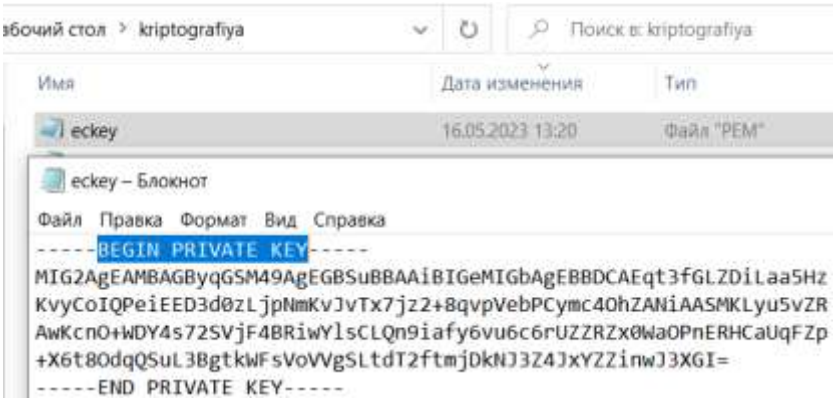
<openssl genpkey -algorithm EC -out eckey.pem -pkeyopt ec_paramgen_curve:P-384 -pkeyopt ec_param_enc:named_curve> - Elliptik egri chiziqqa asoslangan P 384 maydonda kalit hosil qilish.

```
C:\Users\HP\Desktop\kriptografiya>openssl genpkey -algorithm EC -out eckey.pem -pkeyopt ec_paramgen_curve:P-384 -pkeyopt
 ec_param_enc:named_curve

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

16-rasm. Elliptik egri chiziqqa asosida kalit hosil qilish.

Yaratilgan faylni ochib ko'rish(17-rasm).



17-rasm. Elliptik egri chiziqqa asosan OpenSSL da kalit ko'rinishi.

Xulosa

OpenSSL kutubxonasi bir qancha kriptografik algoritmlar asosida maxfiy kalit hamda maxfiy kalit oraliq ochiq (hammaga ma'lum oshkor kalit)

generatsiyasi uchun foydalaniladigan dasturiy vosita bo'lib, undagi buyruqlar orqali har xil kriptografik algortimlardan foydalanish mumkin. Masalan ushbu maqolada kalit generatsiyasi uchun foydalanilgan algoritmlar RSA, DSA algoritmi va DH parametri orqali kalit generatsiyasi, shuningdek, elliptik egri chiziqqa asoslangan kalit generatsiyalash jarayoni kirishi mumkin.

FOYDALANILGAN ADABIYOTLAR:

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

23. Detection of Intrusions and Malware, and Vulnerability Assessment 16th International Conference, DIMVA 2019, Gothenburg, Sweden, June 19–20, 2019, Proceedings

24. Blowfish Cipher Tutorials - Herong's Tutorial Examples, Dr. Herong Yang · 2020

25. Aldaya, A.C, Pereida Garcia, C., Alvarez Tapia, L.M., Brumley, B.B.: Cache-timing attacks on RSA key generation. IACR Cryptology ePrint Archive 2018(367)(2018). https://eprint.iacr.org/2018/367

26. 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.]

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

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

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

30. Internet sayti: https://www.openssl.org/docs/man1.0.2/man1/openssl-genpkey.html