ELLIPTIK EGRI CHIZIQQA ASOSLANGAN DIFFI XELMAN ALGORITMLARI YORDAMIDA KALITLARNI GENERATSIYALASH

I.S.Olimov [1*], A.A.Karimov [2], X.I. Ibrohimov [1]
[1,2,1]Tashkent university of information technologies named after Muhammad al- Khwarizmi
E-mail: karimovabduqodir041@gmail.com

Annotatsiya. *Ushbu maqola elliptik egri chiziqqa asoslangan Diffie-Hellman algoritmlari yordamida kalitlar generatsiyalashning amaliy ta'sirini va xavfsizligini ko'rib chiqadi. Diffie-Hellman (DH) algoritmi, asosiy kriptoqrafik protokollar yaratishda foydalaniladigan mahalliy-mahalliy kalit almashinuv (key exchange) uchun ishlatiladi. Elliptik egri chiziqqa asoslangan Diffie-Hellman (ECDH) algoritmi, DH algoritmini xavfsizroq qilish va tezlashtirish maqsadida kriptoqrafik xavfsizlikni oshiruvchi yangi yondashuvdir. Maqolada ECDH algoritmi tushunchasi, ishlatilishi va amaliy qosimchalar mavjudligi haqida ma'lumot beriladi.*

Kalit so‘zlar. *Elliptik egri chiziq, Diffie-Hellman algoritmi, ECDH, Kalit generatsiyasi, Kriptoqrafik xavfsizlik.*

KIRISH

Kriptoqrafik tizimlarda kalit almashinuv protokollari, muvofiqlashtiruvchi va qabul qiluvchi o'rtasidagi xavfsiz kommunikatsiya uchun zarurdir. Diffie-Hellman (DH) algoritmi, birinchi marta 1976-yilda Whitfield Diffie va Martin Hellman tomonidan ishlab chiqilgan va mahalliy-mahalliy kalit almashinuv (key exchange) uchun asosiy kriptoqrafik protokolga aylangan algoritmdir. Ushbu algoritmda, kommunikatsiya qatnashchilari o'zlarining maxfiy kalitlarini saqlab qolishingiz va ularning jamoat kalitlarini almashishingiz mumkin.

Elliptik egri chiziqqa asoslangan Diffie-Hellman (ECDH) algoritmi, DH algoritmini xavfsizroq qilish va tezlashtirish maqsadida kriptoqrafik xavfsizlikni oshiruvchi yangi yondashuvdir. ECDH algoritmi, o'zining o'ziga xos xususiyatlariga ega bo'lgan elliptik egri chiziqqa asoslangan matematik tushunchalar va algoritmlar ishlatadi.

Elliptik Egri chiziqqa asoslangan Kriptotizimlar

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 [1,5].

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.

ECDH algoritmi, quyidagi bosqichlarda amalga oshiriladi:

Ijrochilar (Alice va Bob) elliptik egri chiziq E va modul p ustida ishlash uchun kelishishadi.

Alice va Bob o'zining maxfiy kalitlarini (a va b) tanlaydi, ularning har biri [1, p-1] oralig'ida bo'lishi kerak.

Alice va Bob o'zining jamoat kalitlarini hisoblash uchun elliptik egri chiziq ustida nuqta ko'paytirish amalini ishlatadi: A = a * G va B = b * G, G elliptik egri chiziqning nuqtasi.

Alice va Bob o'zining maxfiy kalitlari va qabul qilgan jamoat kalitlarini ishlatib, o'zaro kalitni hisoblaydilar: K_Alice = a * B va K_Bob = b * A. Bu yerda, K_Alice va K_Bob bir xil bo'lishi kerak.

Diffie-Hellman protokolining ochiq manbali almashuvlar uchun xavfsizlikni ta'minlashda ishlatilish tartibi quyidagicha:

Foydalanuvchi A va foydalanuvchi B aloqa qiluvchi tomonlarni (p, g) belgilangan o'nlik sanoq sistemasidan olib tashlaydi, masalan, $p = 47$ va $g = 5$.

Foydalanuvchi A a sanoqni o'z maxfiy raqamini tanlaydi, masalan, $a = 7$.

Foydalanuvchi B b sanoqni o'z maxfiy raqamini tanlaydi, masalan, $b = 18$.

Foydalanuvchi A g^a ni hisoblaydi, ya'ni $5^7 = 78,125$**.** Ushbu qiymatni foydalanuvchi B ga yuboradi.

Foydalanuvchi B g^b ni hisoblaydi, ya'ni $5^{18} = 3814697265625$ Ushbu qiymatni foydalanuvchi A ga yuboradi.

Foydalanuvchi A g^b ni hisoblaydi, ya'ni $3814697265625 ^7 \bmod 47 = 34$. Ushbu qiymat umumiy maxfiy kalit sifatida ishlatilishi mumkin.

Foydalanuvchi B g^a ni hisoblaydi, ya'ni $78,125^{18} \bmod 47 = 34$. Ushbu qiymat ham umumiy maxfiy kalit sifatida ishlatilishi mumkin.

Foydalanuvchilar A va B, umumiy maxfiy kalitni ishlatib, aloqalarni shifrlaydilar.

Shaxsiy kalitlar a va b maxfiy sifatida saqlanadi. Foydalanuvchilar aloqalarni shifrlashda, umumiy maxfiy kalit ishlatiladi va aloqalarni shifrlash uchun maxfiylikni ta'minlaydi.

Bu tartibda, foydalanuvchilar o'zmaxfiy raqamlarini boshqa shaxslar bilan almashishda foydalanish mumkin bo'lgan umumiy kalitni ishlatishadi. Foydalanuvchilar aloqalarni shifrlashda, umumiy maxfiy kalit ishlatiladi va aloqalarni shifrlash uchun maxfiylikni ta'minlaydi [2,4].

Natijada, foydalanuvchilar A va B o'zaro xavfsiz aloqada bulishlari mumkin bo'ladi. Shaxsiy kalitlar katta sonlardan olib tashlanib, qattiq faktorlash muammosini hal qilish esa qiyinroq bo'ladi. Shuning uchun, shaxsiy kalitlar olishda, kichik sonlarni ishlatish ko'rsatiladi.

Yuqoridagi misolda, foydalanuvchilar A va B aloqalarni shifrlash uchun umumiy maxfiy kalit sifatida 34 ni ishlatishadi. Ushbu maxfiy kalit boshqa foydalanuvchilar uchun maxfiy emas va aloqa ma'lumotlarini shifrlashda ishlatilmaydi.

ECDH algoritmi xavfsizligi

ECDH (Elliptic Curve Diffie-Hellman) protokoli, ikki tomondoshlar o`rtasida xavfsiz kalit almashishni taminlovchi kriptografik protokol hisoblanadi. Bu protokol eliptik e'rga asoslangan hisoblashlar yordamida ishlashni ta'minlaydi va bu e'rganing matematikaviy xususiyatlaridan foydalanib xavfsizlikni taminlaydi.

ECDH, klassik Diffie-Hellman protokoliga o`xshash tarzda ishlaydi. Ikki tomonning ham birer yolg'on maxfiy kaliti ham birer ochiq kaliti bor. Har bir tomon o'zining ochiq kalitini boshqa tomon bilan almashadi va so'ng maxfiy kalitlarini ishlatib o'rta umumiy kalitni hosil qilishadi. Ushbu umumiy kalit keyingi simmetrik kalitli shifrlash algoritmalarida ishlatilishi mumkin.

ECDH xavfsizligi, eliptik e'rga asoslangan hisoblashlar yordamida ishlashdan kelib chiqadi. Ushbu xususiyatlar ham saldirlar uchun kalitlarni baxtli qirg'ishlariga qarshi himoya qiladi. ECDH, xavfsiz kalit almashishni ta'minlash uchun keng tarqalgan usul hisoblanadi [3,6].

Lekin, ECDH xavfsizligi boshqa faktorlar bilan ham tasir etilishi mumkin, masalan, amaliy qo'llanish va tuzilish xatoliklari kabi. Shuning uchun, protokolni to'g'ri shaklda qo'llash va tuzilish juda muhimdir. Qulay keladigan kalit boshqaruvining, kalit uzunligining va boshqa xavfsizlik chora-tadbirlari kabi yaxshi kriptografik amallarni qo'llash ham muhimmu.

Natijada, ECDH protokoli to'g'ri tarzda qo'llanilganda, xavfsiz kalit almashishni ta'minlash uchun samarali usul hisoblanadi. Lekin, amaliy qo'llanish va tuzilish xatoliklari kabi boshqa faktorlar ham hisobga olinishi kerak.

ECDH algoritmi foydalanishining afzalliklari

ECDH algoritmi, bir nechta afzalliklarga ega:

Xavfsizlik: ECDH algoritmi, ECDLP muammosiga asoslangan xavfsizlik bilan kriptoqrafik tizimlarni ta'minlaydi. Bu, algoritmini kompyuter hujumlari va shifrlarni buzishga qarshi yanada xavfsiz qiladi.

Tezlik: Elliptik egri chiziqqa asoslangan algoritmlar, odatiy DH algoritmidan ancha tezroq ishlaydi. Bu, ECDH algoritmini kommunikatsiya va shifrlash uchun juda samarali qiladi.

Effektivlik: ECDH algoritmi, odatiy DH algoritmidan kamroq resurs va energiya sarflovchi. Bu, ECDH algoritmini mobil qurilmalar, IoT qurilmalari va boshqa resurslar chegaralanuvchi tizimlar uchun juda qo'l keluvchi qiladi.

Diffie-Hellman kriptografik protokoli

Diffie-Hellman kriptografik protokoli, ikki tomondoshlar o`rtasidagi xavfsiz kalit almashishni ta'minlovchi bir usul hisoblanadi. Bu protokol, maxfiy kalit kriptografisidan foydalanib, ikki tomon orasida umumiy kalit hosil qilishni ta'minlaydi.

Diffie-Hellman protokoli, har bir tomonning birer gizli va ochiq kaliti bor. Har bir tomon o'zining ochiq kalitini boshqa tomon bilan almashadi va so'ng maxfiy kalitlarini ishlatib umumiy kalitni hosil qiladi. Ushbu umumiy kalit keyingi simmetrik kalitli shifrlash algoritmalarida ishlatilishi mumkin.

Diffie-Hellman protokolining xavfsizligi, modulyar arifmetik hisoblashining matematikaviy xususiyatlaridan kelib chiqadi. Ushbu xususiyatlar saldirlarga qarshi kalitni baxtli qirg'ishlariga qarshi himoya qiladi.

Lekin, Diffie-Hellman protokoli xavfsizligi boshqa faktorlar bilan ham tasir etilishi mumkin, masalan, amaliy qo'llanish va tuzilish xatoliklari kabi. Shuning uchun, protokolni to'g'ri shaklda qo'llash va tuzilish juda muhimdir. Qulay keladigan kalit boshqaruvining, kalit uzunligining va boshqa xavfsizlik chora-tadbirlari kabi yaxshi kriptografik amallarni qo'llash ham muhimmu.

Natijada, Diffie-Hellman protokoli to'g'ri tarzda qo'llanilganda, xavfsiz kalit almashishni ta'minlash uchun samarali usul hisoblanadi. Lekin, amaliy qo'llanish va tuzilish xatoliklari kabi boshqa faktorlar ham hisobga olinishi kerak.

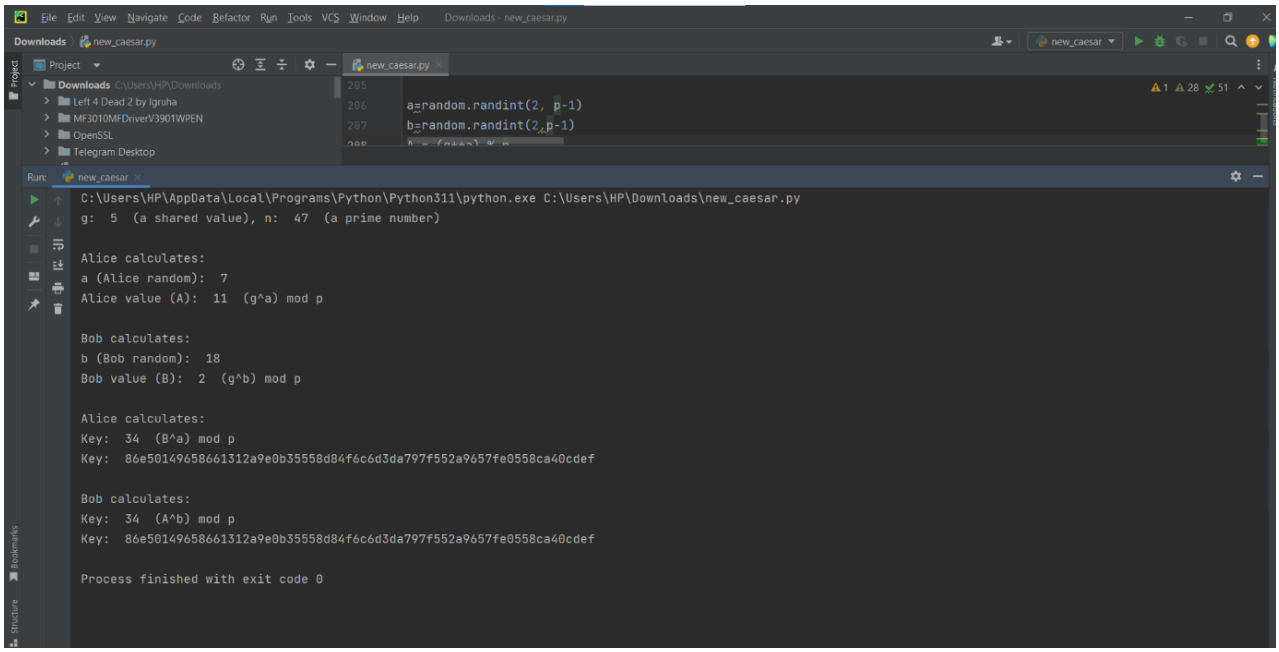
Quyidagi misolni ishlab ko‘rishimiz mumkin dastur orqali:

p = 47 va g = 5 bo'lsin. Har qanday ikkita raqamni ikkita aloqa qiluvchi tomonning shaxsiy kalitlari sifatida oling va ular umumiy kalitni umumiy maxfiy kalit sifatida qanday olishlarini ko'rsating.

```
import random
import hashlib
import sys
g=5
p=47
a=random.randint(2, p-1)
b=random.randint(2,p-1)
A = (g**a) % p
B = (g**b) % p
```

```
print('g: ',g,' (a shared value), n: ',p, ' (a prime number)'
print('\nAlice calculates:')
print('a (Alice random): ',a)
print('Alice value (A): ',A,' (g^a) mod p'
print('\nBob calculates:')
print('b (Bob random): ',b)
print('Bob value (B): ',B,' (g^b) mod p')
print('\nAlice calculates:')
keyA=(B**a) % p
print('Key: ',keyA,' (B^a) mod p')
print('Key: ',hashlib.sha256(str(keyA).encode()).hexdigest())
print('\nBob calculates:')
keyB=(A**b) % p
print('Key: ',keyB,' (A^b) mod p')
print('Key: ',hashlib.sha256(str(keyB).encode()).hexdigest())
```

Natija:



Xulosa

Elliptik egri chiziqqa asoslangan Diffie-Hellman (ECDH) algoritmi, asosiy kriptoqrafik protokollar yaratishda foydalaniladigan kriptoqrafik xavfsizlikni oshiruvchi yangi yondashuvdir. Ushbu maqola ECDH algoritmi tushunchasi, ishlatilishi va amaliy qosimchalar mavjudligi haqida ma'lumot beradi. ECDH algoritmi, kriptoqrafik xavfsizlik, tezlik va effektivlik jihatidan odatiy Diffie-Hellman algoritmidan afzaldir. ECDH algoritmi, mobil qurilmalar, IoT qurilmalari va boshqa resurslar chegaralanuvchi tizimlar uchun juda qo'l keluvchi ekanligini ko'rsatadi.

FOYDALANILGAN ADABIYOTLAR

1. Lara-Nino, Carlos Andres, Arturo Diaz-Perez, and Miguel Morales-Sandoval. "Lightweight elliptic curve cryptography accelerator for internet of things applications." *Ad Hoc Networks* 103 (2020): 102159.

2. Ibrahim, Saleh, and Ayman Alharbi. "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography." *IEEE Access* 8 (2020): 194289-194302.

3. IK, Yusupova SM AmonovA H. Abdullayev, and M. A. Avazbekov. "OPENSSL KUTUBXONASIDA ELLIPTIK EGRI CHIZIQQA ASOSLANGAN DIFFI-XELMAN ALGORITMI." *INNOVATION IN THE MODERN EDUCATION SYSTEM* 3.30 (2023): 525-532.

4. Yusupova, S. M. "ELLIPTIK EGRI CHIZIQQA ASOSLANGAN KRIPTOTIZIMLAR." *INNOVATION IN THE MODERN EDUCATION SYSTEM* 3.30 (2023): 533-541.

5. Bashir, Zia, et al. "Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol." *Multimedia Tools and Applications* 81.3 (2022): 3867-3897.

6. Ametepe, A. F. X., Ahouandjinou, A. S., & Ezin, E. C. (2022). Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks. *Wireless Networks*, *28*(3), 991-1001.