FERMAT FAKTORLASH USULI

Rashidova Oydinoy Jo‘rabek qizi
TATU akademik litseyi

Annotatsiya. *Ushbu maqolada sonlar nazariyasining klassik usullaridan biri — Fermat faktorlash algoritmining matematik modeli va uning zamonaviy kriptotahlildagi o‘rni tadqiq etiladi. Fermat usuli ko‘paytuvchilar bir-biriga yaqin bo‘lgan hollarda an’anaviy metodlardan sezilarli darajada ustunlikka ega.*

Kalit so‘zlar*: Fermat usuli, tub sonlar, sonlar nazariyasi, faktorlash*

KIRISH

Zamonaviy axborot xavfsizligi tizimlari, xususan RSA algoritmi, katta butun sonlarni ko‘paytuvchilarga ajratishning (faktorlash) hisoblash nuqtai nazaridan qiyinligiga asoslangan. Faktorlash muammosini yechish uchun ko‘plab algoritmlar mavjud bo‘lib, ular orasida Pyer Fermat tomonidan XVII asrda taklif etilgan usul alohida o‘rin tutadi. Ushbu bo‘limda faktorlashning dolzarbligi va Fermat usulining tarixiy ahamiyati bayon etiladi.

Axborotni kriptografik himoya qilishda asimmetrik shifrlash algoritmlari, xususan RSA, tub sonlarni ko‘paytirishning osonligi va hosil bo‘lgan murakkab sonni faktorlashning qiyinligiga asoslanadi. Faktorlash muammosi — NP-murakkab masalalar sinfiga yaqin bo‘lib, uni yechishning samarali usullarini izlash kiberxavfsizlikning dolzarb yo‘nalishidir. Pyer Fermat tomonidan taklif etilgan faktorlash usuli, trial division (ketma-ket bo‘lish) usulidan farqli o‘laroq, sonning strukturaviy xususiyatlariga — kvadratlar ayirmasiga asoslanadi.

METODOLOGIYA

Fermat faktorlash usuli berilgan n toq sonini ikki kvadrat ayirmasi ko‘rinishida yozish mumkinligi haqidagi Fermat teoremasiga asoslanadi:

$$n = x^2 - y^2, x \; va \; y \; butun \; sonlar$$

Bu ifodani $n = (x - y)(x + y)$ ko‘rinishida ifodalash orqali, $p = x - y$ va $q = x + y$ aniqlanadi.

Algoritmning qadamlari quyidagi tartibda ishlaydi: $x = [\sqrt{n}]$ qiymatidan boshlab, $y^2 = x^2 - n$ ayirma hisoblanadi.Agar y^2 to‘la kvadratga ajralsa, algoritm to‘xtaydi. Shart bajarilmagan taqdirda, x ning qiymati 1 ga oshiriladi va shu sikl davom etadi.

$$x = \frac{p+q}{2} \; va \; y = \frac{-p+q}{2}$$

Agar p va q sonlari bir-biriga juda ham yaqin bo‘lsa, x ning qiymati $\sqrt{n}$ ga yaqin keladi.

NATIJALAR

Fermat usulini samaradorligini sinash uchun n=8051 sonini misol qilaylik. Boshlang‘ich nuqtani aniqlash uchun n sonidan kvadrat ildiz chiqaramiz.

$$\sqrt{8051} \approx 89.7$$

Demak, tajribani 90 dan boshlaymiz: $x = 90$

Algoritmning har bir iteratsiyasida $y^2 = x^2 - n$ ayirma tekshirib ko‘riladi.Ammo hozirgi holatda, $x^2 - n = 90^2 - 8051 = 49$. 49 soni esa 7 ning kvadrati hisoblanadi.

x=90 va y=7 ga teng ekanligini topdik. Bu orqali p va q ni topishimiz mumkin: p=x-y=90-7=83 va q=x+y=90+7=97. Tekshirsak, 8051=83x97. Haqiqatda ham to‘g‘ri.

Ko‘rinib turibdiki, Fermat usulida bitta urinishda 8051 sonini ikkita tub son ko‘rinishda ifodalash mumkin. Endi an’anaviy usul- bo‘lib chiqish usulida esa, 8051 sonini 2 dan 89 gacha(8051 ning kvadrat ildiziga eng yaqin tub son) bo‘lib chiqish kerak. Bu 83 soniga kelganda to‘xtaydi va ungacha 23 marta amal bajaradi.

Endi tajribani 1649 soni bilan davom ettiraylik:

$$\sqrt{1649} \approx 40.6$$

1-jadval. Iteratsiya jarayoni

Iteratsiya(qadam)	x	y^2
1	41	32
2	42	115
3	43	200
4	44	287
5	45	376
6	46	467
7	47	560
8	48	655
9	49	752
10	50	851
11	51	952
12	52	1055
13	53	1160
14	54	1267
15	55	1376
16	56	1487
17	57	1600

Jadvaldan ma’lumki, 17-qadamga kelib, y^2 to‘la kvadratga ajraldi.$x = 57$ va $y = 40$ ga teng ekan. p va q ni topsak, ular 17 va 97 ekanligi kelib chiqadi.

Bu misol shuni ko‘rsatadiki, Fermat usul ko‘paytuvchilar bir-biridan ancha uzoq bo‘lsa, ko‘proq iteratsiya talab qiladi.

XULOSA

Tadqiqot natijalari shuni ko‘rsatadiki, Fermat usuli barcha turdagi sonlar uchun universal samarali yechim bo‘la olmaydi. Tajribalar davomida aniqlanishicha, ko‘paytuvchilar p va q bir-biridan raqamlar o‘qida uzoq joylashgan hollarda algoritmdagi iteratsiyalar soni keskin ortib boradi va hisoblash samaradorligi pasayadi. Shunga qaramay, ushbu metod bugungi kunda eng tezkor hisoblangan Kvadratik elak kabi zamonaviy faktorlash algoritmlari uchun fundamental matematik baza bo‘lib xizmat qiladi.

Xulosa qilib aytganda, Fermat faktorlash usuli o‘zining matematik soddaligiga qaramay, zamonaviy kiberxavfsizlikda hamon dolzarb ahamiyatga ega. U bizga shifrlash kalitlarini yaratishda nafaqat tanlanayotgan sonlarning "tub" bo‘lishi, balki ularning bir-biriga nisbatan joylashuvi ham xavfsizlikning muhim mezoni ekanligini isbotlaydi. Bu esa RSA kabi asimmetrik shifrlash tizimlarining mustahkamligini ta'minlashda metodologik asos bo‘lib xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. G‘aniyev, S. K., & G‘aniyev, A. S. (2019). Kriptografik usullar va axborot xavfsizligi. Toshkent: "O‘qituvchi".
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th Edition). Pearson.
3. Koblitz, N. (1994). A Course in Number Theory and Cryptography. Springer-Verlag.
4. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.