TUB SONLARGA ASOSLANGAN ASSIMMETRIK KRIPTOTIZIMLAR UCHUN KATTA TUB SONLARNI GENERATSIYALASH VA ULARNI TUBLIKKA TEKSHIRISH ALGORITMLARI TADQIQ QILISH

Salayev Alisher Kuralbayevich
salayevalisher@gmail.com
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalar
universiteti Urgnch filiali

Annatatsiya: Ushbu maqola assimmetrik kalitli kriptografik algoritmlarida keng qo‘llaniladigan katta tub sonlarni generatsiya qilish va tublikka tekshirish algoritmlarining samaradorligi, afzalliklari va kamchiliklari tadqiqiga bag‘ishlangan.

Kalit so‘zlar: Katta tub son, tub son generatori, tublikka tekshirish testi, tub sonlar konsentratsiyasi.

Annotation: This article is devoted to the study of the effectiveness, advantages and disadvantages of large prime number generation and cardinality checking algorithms, which are widely used in asymmetric key cryptographic algorithms.

Key words: Large prime number, prime number generator, primeness test, concentration of prime numbers.

KIRISH

Zamonaviy kriptografiya, shu jumladan kalitlarni taqsimlash kriptografik protokollari barchasi matematik muammolarning maxsus sinflari atrofida ishlab chiqilgan bo‘lib, ularni yechish amaliy jihatdan “qiyin” hisoblanadi. Hisoblash murakkabligi gipotezasi shuni ko‘rsatadiki, ma’lum bir muammoni bugungi texnologiyalari va hisoblash resurslari yordamida samarali hal qilib bo‘lmaydi. Bu yerda “samarali” iborasi “oqilona vaqt ichida” manosida ishlatilmoqda. Muammoni hal qilish uchun zarur bo‘lgan vaqt miqdori (ya’ni, ba’zi bir kirish parametrlari berilganda chiqish natijasini topishga sarflangan vaqt) - bu kirish parametrining o‘lchamidan osongina baholanadigan miqdor. Odatda, kirish hajmi qanchalik katta bo‘lsa, muammoni hal qilish uchun zarur bo‘lgan vaqt miqdori shunchalik katta bo‘ladi. Ammo, agar natija olish vaqti kirish hajmining eksponensial funksiyasi bo‘lsa, unda nisbatan kichik o‘zgarish ham muammoni hal qilish uchun bir necha milliard yillarni talab qiladi. Binobarin, amaldagi texnologiyalar va algoritmlardan foydalangan holda eksponensial vaqtni saralashni talab qiladigan muammolar hisoblash uchun "qiyin" hisoblanadi[2].

ADABIYOTLAR TAHLILI VA METODLAR

Misol tariqasida, eng taniqli ochiq kalitli kriptotizim RSA ni qaraydigan bo‘lsak, berilgan butun sonning asosiy faktorizatsiyasini hisoblash murakkabligiga asoslangan. Ushbu muammoni hal qilish uchun ma’lum algoritm eksponensial vaqt hisoblanishini talab etadi, shu sababli tavsiya etilgan ochiq kalit hajmi 1024, 2048 va 3072 bit bo‘lsa RSA kriptotizimi xavfsiz hisoblanadi. Chunki bugungi kunda dushman potensiali odatdagi hisoblash kuchi va resurslar bilan hisoblanadi. Biroq, bu hozirgi tajribaga asoslangan taxmin, chunki muammoni printsipial ravishda buzish mumkin emasligi to‘g‘risida matematik dalillar mavjud emas, masalan, hali kashf etilmagan boshqa algoritm bilan[2].

Yuqorida keltirilgan darajada xavfsizlikni ta’minlash uchun o‘z-o‘zidan talab qilingan darajada katta tub sonlarni generatsiya qilish yoki katta sonlarni tublikka tekshirish muammosi yuzaga chiqadi.

Hozirgi kunda katta ehtimol bilan tub sonlarni generatsiya qilishning nir necha usullari mavjud, quyida ular bilan atroflicha tanishib o‘tamiz.

1-usul. Tub sonlarning dastlabki ikkitasi 2 va 3 lardan tashqari barchasi $6n-1$ yoki $6n+1$ bunda $(n \in N)$ ketma-ketliklarning hadi hisoblanadi. Bu ketma-ketliklarning ustun tarafi tub sonlar qatoridagi barcha tub sonlarni o‘z ichiga olishi bo‘lsa, kamchilik taraflaridan biri n soni kattalashib borgani sari ketma-ketlik hadlari orasida tub sonlar konsentratsiyasi kamayib boradi. Buni quyida keltirilgan 1-jadvalda yaqqol ko‘rishimiz mumkin. Bu va bundan keyin keltirilgan jadvallardagi ma’lumotlar va natijalar quyida keltirilgan algoritm bo‘yicha hisoblangan.

```
Function tub(n){
        Flag = false
        If  n-tub then flag = true
Return(flag)
}
For  i in range(1,m)
        If tub(f(i)) then k++; //f(i) – berilgan usullardagi ketma-ketlik qoidasi;
Print(k) //k – dastlabki m ta hadlari ichidagu tub sonlar soni;
```

1-jadval

Hadlar soni	10	100	1000	10000	100000
Konsentratsiyasi	90%	62%	42,9%	32,43%	25,995%

1-usul yordamida hosil qilingan hosil qilingan sonlarning tub sonlari konsentratsiyasi jadvali

2-usul. 40 da katta ba’zi tub sonlar n^2+n+41 $(n=0,1,2,\dots)$ ketma-ketlikning hadlari bo‘lishi mumkin. Albatta bu ketma-ketlikning barcha hadi tub son emas, bunga yaqqol dalil agar n soni 41 ga karrali bo‘lsa uning natijasi 41 ga karrali

bo‘ladi. Bundan boshqa hollarda ham murakkab son chiqishi mumkin. Bu usulda tub sonlar konsentratsiyasini quyidagi 2-jadvalda ko‘rishimiz mumkin.

2-jadval

Hadlar soni	10	100	1000	10000	100000
Konsentratsiyasi	100%	86%	58,1%	41,48%	31,984%

2-usul yordamida hosil qilngan hosil qilingan sonlarning tub sonlari konsentratsiyasi jadvali

3-usul. Mersenning tub sonlari. $M_p = 2^p - 1 \quad (p = 2,3,4, \dots)$ Oldingi usullardagi kabi bu ketma-ketlikning ham barcha hadi tub son emas. 3-jadvalda Mersenning tub sonlari konsentratsiyasini keltirib o‘tamiz.

3-jadval

Hadlar soni	10	50	60
Konsentratsiyasi	40%	16%	15%

3-usul yordamida hosil qilngan hosil qilingan sonlarning tub sonlari konsentratsiyasi jadvali

4-usul. Fermaning tub sonlari. $F_p = 2^{2^p} + 1 \ (p \in N)$ Oldingi usullardagi kabi bu ketma-ketlikning ham barcha hadi tub son emas. 4-jadvalda Mersenning tub sonlari konsentratsiyasini keltirib o‘tamiz.

4-jadval

Hadlar soni	5	6	7
Konsentratsiyasi	80%	66,67%	57,14%

4-usul yordamida hosil qilngan hosil qilingan sonlarning tub sonlari konsentratsiyasi jadvali

Yuqorida ko‘rib o‘tgan usullarimizga e’tibor qaratadigan bo‘lsak ketma-ketliklarni hadlari kattalashgani sari hosil qilingan sonning tub bo‘lish ehtimoli kamayib boradi. Bunda kelib chiqadiki, ko‘rib chiqilgan yoki boshqa usullar yordamida hosil qilingan sonlardan foydalanish va amaliyotga tadbiq qilish uchun ularni tublikka tekshirish kerak bo‘ladi.

Birzga ma’lumki oliy matematika kursida sonning tubligini aniqlovchi o‘z isbotini topgan teotema mavjud, yani:

Teorema: Ixtiyoriy $n, \ (n \in N)$ son tub bo‘lishi uchun o‘zining kvadrat ildizi butun qismigacha bo‘lgan tub sonlarga karrali bo‘lmasligi zarur va yetarli.

Bu teorema berilgan sonni tub yoki murakkabligini aniqlaydigan eng optimal usullaridan bo‘lishiga qaramasdan juda katta sonlarni testlashda ko‘p vaqt va resurs talab qilishi mumkin, bundan tashqari berilgan son testlanish jarayonida bir qancha resurslar sarflanganidan keyin muvaffaqiyatsizlikka uchrasa sarflangan resurslar bekorga isrof bo‘ladi. Misol uchun biror katta
sonni testlashda uning ildizigacha bo‘lgan tub sonlar 2000 ta bo‘lsa vas hu sonlarga bo‘lib ko‘rish jarayoni boshlangandan keyin 987-o‘rindagi tub songa bo‘linish bajarilsa, undan oldingi 986 ta tub songa bo‘lib tekchirish uchun sarflangan vaqt va boshqa resurslar isrof bo‘ladi.

Shu va shunga o‘xshash isrofgarchiliklarning oldini olish uchun sonni to‘liq tublikka tekshirishdan oldin tub bo‘lish ehtimoli yuqori bo‘lgan sonlarni tanlashimiz kerak bo‘ladi. Buni amalga oshirishda biz yuqoridagi yoki shunga o‘xshash tub bo‘lish ehtimoli bo‘lgan sonli ketma-ketliklarda va sonlarni tublikka tekshirish testlarida foydalanishimiz mumkin.

Sonlarni tublikka tekshirish testlarini ko‘rib chiqamiz.

Albatta sonlarni murakkab tublik testlaridan o‘tkazishdan oldin kichik tub sonlarga bo‘linish belgilari yordamida ularga bo‘linish yoki bo‘linmasligini tekshirib ko‘rishimiz maqsadga muvofiq. Masalan: 2 ga, 3ga, 5 ga, 7 ga, 11 ga va h.k.

Ferma testi: Agar $a < n$ $(a \in N)$ va n tub son bo‘lsa

$$a^{n-1} \equiv 1 mod n$$

tenglik o‘rinli bo‘ladi.

Mazkur usul yozdamida berilgan berilgan n sonni tubligini testdan o‘kazishimiz mumkin, lekin yuqoridagi tenglik n faqat tub bo‘lgandagina bajarilmaydi. n murakkab bo‘lgan ayrim hollarda ham bajarilishi mumkin. Misol uchun $2^{561-1} = 2^{561} \equiv 1 mod 561$ $(561 = 3 \cdot 11 \cdot 17)$. Bundan ko‘rinadiki Ferma testi berilgan sonning tub bo‘lish ehtimolinitekshiradi xalos.

Rabin-Miller testi: Bu testlash usulini Ferma testining umulashgan shakli sifatida tushinsak bo‘ladi. Mazkur usul uchun testlash formulasi quyidagi ko‘rinishga ega.

$$a^m \equiv \pm 1 mod n, \;\; n-1 = 2^k \cdot m \qquad \text{bu yerda } k, m \in N$$

bu usulda berilgan sonni tublikka tekshirish uchun berilgan n sonidan 1 kamaytiriladi va natijadan bo‘lishi mumkin bo‘lgan 2 ning eng katta darajasi (2^k) ajratib olinadi va qolgan qismi (m) orqali testdan o‘tkaziladi. Yani, agar $a^m \equiv \pm 1 mod n$ tenglik bajarilsa berilgan sonning tub bo‘lish ehtimolligi yuqori bo‘ladi.

Afsuski, yuqorida ko‘rib chiqilgan testlash usullari, sinovdan muvaffaqiyatli o‘tgan sonlarning barchasi tub bo‘lishi haqida to‘liq kafolat bera olmaydi.

Misol uchun $n = 2047$ sonini tekshiradigan bo‘lsak:

Ferma testi: $2^{2047-1} = 2^{2046} \equiv 1 mod 2047$ bu tenglik bajarildi, ya’ni son Ferma testidan o‘tdi.

Rabin-Miller testi: $2047 - 1 = 2046 = 2^1 \cdot 1023$ ya’ni $m = 1023$ ga teng, $2^{1023} \equiv 1 mod 2047$ bu shart ham bajarildi lekin $(2047 = 23 \cdot 89)$ berilgan son murakkabligini ko‘rishimiz mumkin.

Shu o‘rinda bir savol tug‘ilishu mumkin, aslida natural sonlar qatorida tub sonlar ulushi qanday? Sonlar kattalashgani sari konsentratsiyasi qanday o‘zgaradi? Teng taqsimlanganmi? Bu kabi savollarga quyida keltirilga 5-jadvaldan javob olishimiz mumkin.

5-jadval

Hadlar soni	10	100	1000	10 ming	100 ming	1 mln	10mln
Konsentratsiyasi	40%	25%	16,7%	12,29%	9,592%	7,8498%	6,64579%

XULOSA

Yuqoridagi 5-jadvaldan ko‘rinib turibdiki, natural sonlar qatori kattalashib borgani sari undagi tub sonlar konsentratsiyasi kamayib bormoqda, bu esa o‘z navbatida bizga katta tub sonlarni topishda ancha murakkabliklarni keltirib chiqarishi mumkin.

Albatta tub sonlarni topishda va amaliy masalalarda qo‘llashda sonning tubligini to‘la kafolatlaydigan algoritmlarda foydalaniladi. Bu degani, yuqorida biz ko‘rib chiqqan tun sonlarni generatsiyalash algoritmlari va tanlangan sonlarni tublikka tekshirish testlaridan foydalanilmasligi kerak degani emas. Kafolatlangan tublikka tekshirish algoritmlari ko‘p resurs talab qilganligi uchun, resurslarni tejash maqsadida taklif qilingan tun sonlarni generatsiyalash algoritmlari va tanlangan sonlarni tublikka tekshirish testlaridan foydalanib tub bo‘lish ehtimoli yuqori bo‘lgan sonlarni saralashda ishlatilishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. R. Sh Karimov, A.K Salayev, Implementation of blockchain technologies in the nonfinancial area, Science and Education 2021-yil 2 (5), 310-313bet
2. A.K Salayev, Kvant kompyuterlari va ularning zamonaviy kriptografiyaga tahdidi
   Ilmiy tadqiqot va innovatsiya, 27-29
3. M.M.Aripov, B.F.Abdurahimov, A.S.Matyakubov, Kriptografik usullar, Toshkent 2020

4. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtayeva, Kriptografiyaning matematik asoslari, Toshkent – 2018
5. https://www.programiz.com/python-programming/online-compiler/
6. https://en.wikipedia.org/wiki/Generation_of_primes
7. https://en.wikipedia.org/wiki/Primality_test