XXI ASRDA INNOVATSION TEXNOLOGIYALAR, FAN VA TA'LIM TARAQQIYOTIDAGI DOLZARB MUAMMOLAR
*Volume 03, Issue 04, 2025*

# REKURSIV FUNKSIYA YORDAMIDA TAKOMILLASHTIRILGAN KRIPTOBARDOSHLI KALIT GENERATSIYALASH ALGORITMI VA UNING DASTURI

**Allanazarova Davlatoy Farxod qizi**
Termiz davlat universiteti, Kompyuter tizimlari va ularning dasturiy ta'minoti mutaxassisligi magistranti

**Annotatsiya:** Ushbu maqolada Rabin–Miller algoritmiga asoslangan tublikka sinash metodikasi takomillashtirilib, rekursiv funksiyalar yordamida kriptobardoshli kalit generatsiyasining samaradorligi oshirildi. Taklif etilgan 1*-algoritmda murakkab sonlarni aniqlash aniqligi oshgan bo'lib, "soxta guvohlar" sonini keskin kamaytirish orqali algoritm xavfsizligini kuchaytirishga erishilgan. Takomillashtirilgan algoritm Microsoft Visual Studio 2008 muhitida, C# dasturlash tilida ishlab chiqildi. Dastur MPFR/MPIR kutubxonasi yordamida katta sonlar ustida amallarni amalga oshiradi. Natijalar takomillashgan algoritmning samaradorligi va xavfsizlik darajasi yuqoriligini tasdiqlaydi.

**Kalit so'zlar:** Rabin–Miller testi, rekursiv funksiyalar, kriptobardoshlik, kalit generatsiyasi, soxta guvohlar, C# dasturlash tili, MPFR/MPIR kutubxonasi, axborot xavfsizligi

Rabin – Millerning katta sonlarni tublikka sinash testi hozirgi kunda nosimmetrik kriptotizimlarda modul hosil qilishda keng qo'llaniladi. Bu algoritm kuchli psevdotub sonlarni sinash algoritmi sifatida tan olingan. U $n-1$ ni, ya'ni modulni bitta kamaytirilgan qiymatini $2^s*r$ ko'rinishda ifodalashga asoslangan. Bunda $s$ — $n-1$ ni ikkiga bo'linishlar soni, $r$ – toq son.

**1-algoritm.**

Kirish: Toq butun son $n \geq 3$ va maxfiy parametr $t \geq 1$.

Chikish: "$n$ - soni tubmi?" degan savolga, "tub" yoki "murakkab" degan javob.

1. $n-1 = 2^s*r$ ko'rinishda yozib olinadi, bunda $r$ - tub son.
2. $i$ 1 dan $t$ gacha o'zgarganda quyidagilar bajariladi:
   2.1. $2 \leq a \leq n-2$ shartni qanoatlantiruvchi $a$ son tasodifiy tanlanadi.
   2.2. $u=a^r \mod n$ ni hisoblanadi.
   2.3. Agar ($u \neq 1$ va $u \neq n-1$) bo'lsa, u holda quyidagilar bajariladi:
   $j \leftarrow -1$.

Toki ($j \le s-1$ va $u \ne n-1$) shart o'rinli bo'lsa, quyidagilar bajariladi:

$u \leftarrow u^2 \bmod n$ hisoblanadi.

Agar ($u=1$) bo'lsa, u holda "murakkab son" qaytariladi.

$j \leftarrow\!\!- j+1$.

Agar ($u \ne n-1$) bo'lsa, u holda "murakkab son" qaytariladi.

3. "Tub son" qaytariladi.

Endi ushbu Rabin-Miller testini ko'rib o'tilgan faktorli rekursiv funktsiyani hisoblash algoritmi asosida quyidagicha takomillashtirish mumkin.

**1*-algoritm.**

Kirish: Toq butun son $n \ge 3$ va maxfiy parametr $t \ge 1$.

Chiqish: " $n$ - soni tubmi?" degan savolga, "tub" yoki "murakkab" degan javob.

1. $j \leftarrow 1$, $D_1 \leftarrow a$ ni olinadi.

2. $n-1=2^{s*}r$ ko'rinishda yozib olinadi, bunda $r$ - tub son.

3. $i$ 1 dan $t$ gacha o'zgarganda quyidagilar bajariladi:

3.1. $2 \le a \le n-2$ shartni qanoatlantiruvchi $a$ sonini tasodifiy tanlanadi.

3.2. $y=a^r \bmod n$ hisoblanadi.

3.3. Agar ($u \ne 1$ va $u \ne n-1$) bo'lsa, u holda quyidagilar bajariladi:

$r \leftarrow -1$.

Toki ($r \le s-1$ va $u \ne n-1$) shart o'rinli bo'lsa, quyidagilar bajariladi:

$u \leftarrow u^2 \bmod n$ hisoblanadi.

Agar ($u=1$) bo'lsa, u holda "murakkab son" qaytariladi.

$r \leftarrow r+1$.

Agar ($u \ne n-1$) bo'lsa, u holda "murakkab son" qaytariladi.

3.4 Toki ($D_j \ne n-1$ || $j \ne k$) shart bajarilganda quyidagilar bajariladi:

3.4.1 $D1_j \leftarrow D_j+1$, $a1 \leftarrow j+a$,

$D2_j \leftarrow D1_j * a1$, $D_{j+1} \leftarrow D_j + D2_j$ .

3.4.2 $D_{j+1} \leftarrow \lfloor D_{j+1} / n \rfloor$.

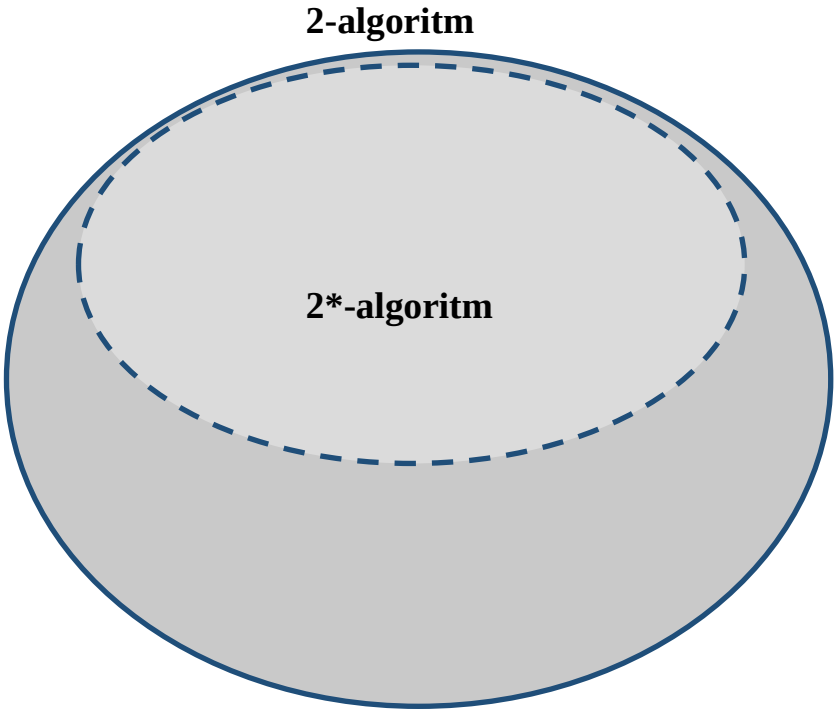
3.4.3 $j{+}{+}$.

3.5 $a \leftarrow D_j$

3.6 $i \leftarrow i+j$.

4. "Tub son" qaytariladi.

Takomillashtirilgan 1* algoritm unga tegishli mavjud algoritmga nisbatan $n$ soni murakkab son bo'lganda uni avvalroq payqab, tublikka "soxta guvohlar" sonini kamaytiradi. Bu quyidagi Venn diagrammasida tasvirlangan (1-rasm).




1-rasm. Mavjud va takomillashtirilgan algoritmning $n$ murakkab son bo'lganda "soxta guvohlar"i egallagan sohalari

Unda "soxta guvohlar" egallagan sohalar uchun tegishli algoritm raqami ko'rsatilgan. Bundan ko'rinadiki, takomillashtirilgan 1*-algoritm hozirgacha ma'lum bo'lgan va eng keng qo'llaniladigan va AQSh standarti [15] uchun asos qilib olingan Rabin-Miller algoritmiga nisbatan ham samaradorlidir, chunki bu algoritm katta tub sonlarni sinashda hosil bo'ladigan "soxta guvohlar" ni keskin kamaytirish imkoniyatini beradi.

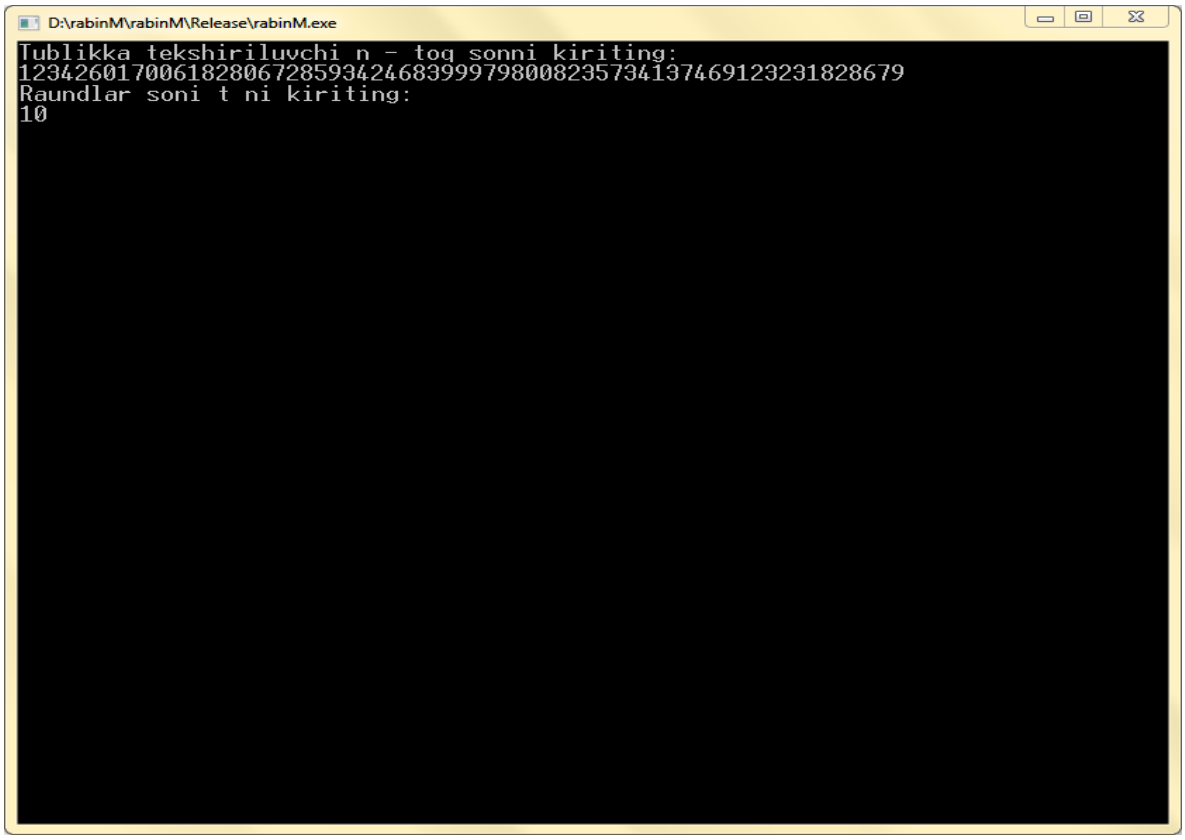
Mazkur magistrlik dissertatsiya ishida rekursiv funktsiyani qo'llash asosida kriptobardoshli kalit generatsiyalashning takomillashgan Rabin-Miller algoritmi ishlab chiqildi. Ushbu algoritmning dasturini yozishda hozirda eng keng qo'llanilayotgan C# («Si sharp») dasturlash tilidan foydalanilgan.

C# dasturlash tili 2000 yilda Maykrosoft kompaniyasi tomonidan ishlab chiqilgan. U Maykrosoft kompaniyasining yangi **.NET** («DotNet») texnologiyasining bir qismi bo'ldi. Ushbu texnologiyalar doirasida turli dasturlash tillarida yozilgan dasturlarni bajarilishining yagona muhiti ko'zda tutilgan. C# - sodda, zamonaviy, xavfsiz tip tizimli ob'ektga yo'naltirilgan. Yuqorida keltirilganlarni inobatga olgan holda taklif etilayotgan kriptobardoshli kalit generatsiyalashning takomillashgan Rabin-Miller algoritmining dasturi Microsoft Visual Studio 2008 muhitida C# dasturlash tilida tuzildi. C# dasturlash tilining boshqa dasturlash tiliga nisbatan tezkor va mobil bo'lganligi sababli algoritm uchun shu dasturlash tili tanlab olindi.

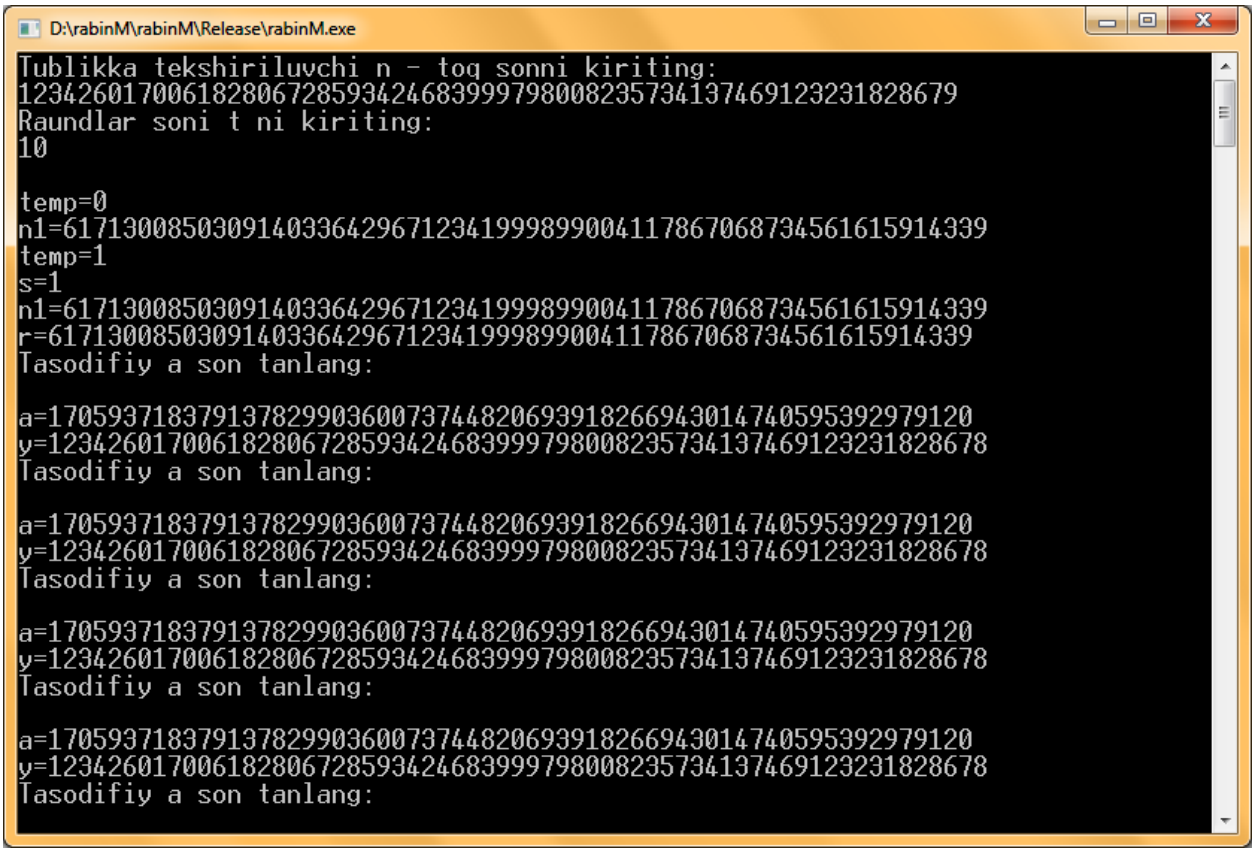
Dastur ilovasini tuzishda MPFR/MPIR kutubxonasidan foydalanildi. MPFR/MPIR kutubxonasi kriptografik protokollar bilan ishlash uchun mo'ljallangan ochiq kodli kriptografik paket hisoblanadi. Bu paket katta butun tub sonlar va ular ustidagi amallarni o'z ichiga oladi. Bu kutubxona C++ tilida yozilgan bo'lib, bu paketni UNIX oilasiga mansub hamda OpenVMS va Microsoft Windows kabi operatsion tizimlarda ham qo'llash mumkin.

***Takomillashgan tublikka sinashning Rabin Miller algoritmi dasturi oynalari*** quyidagi 2–5-rasmlarda keltirilgan.

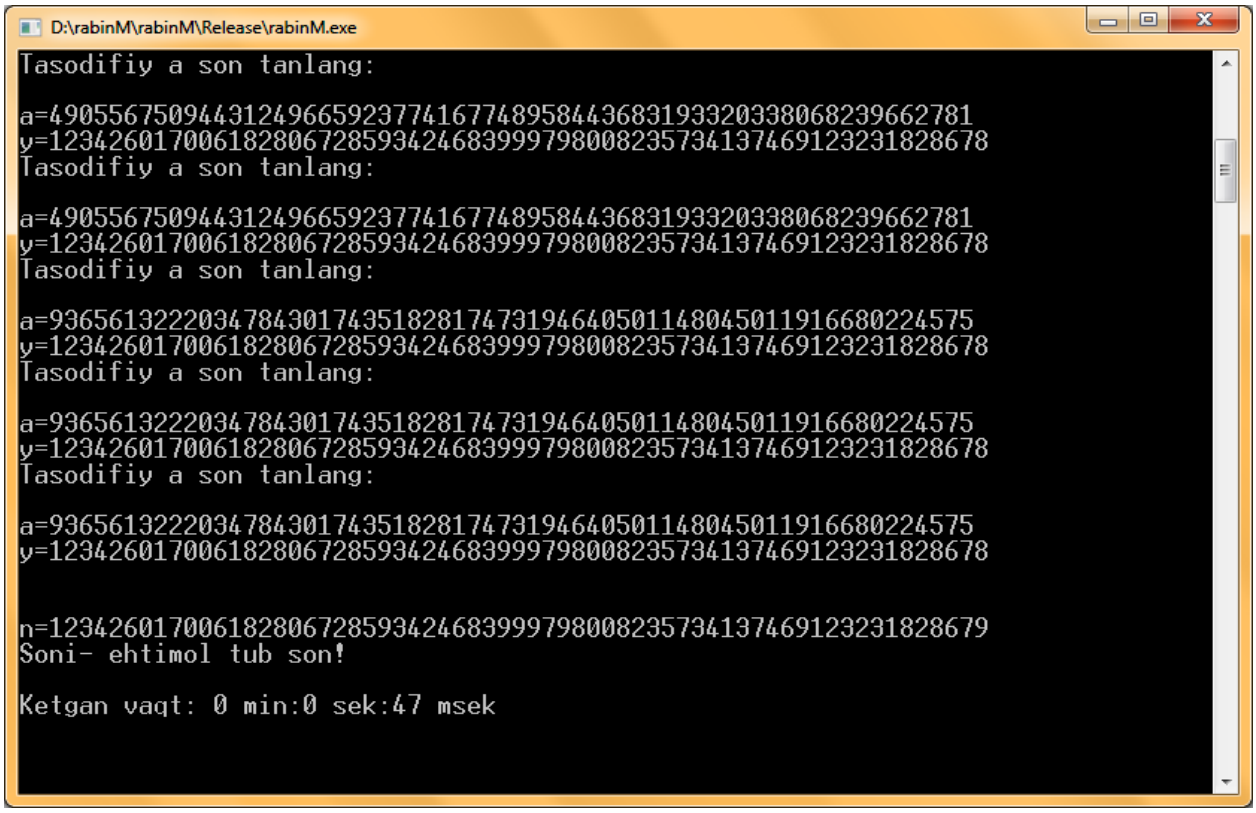

2-rasm


D:\rabinM\rabinM\Release\rabinM.exe
Tublikka tekshiriluvchi n - toq sonni kiriting:
123426017006182806728593424683999798008235734137469123231828679
Raundlar soni t ni kiriting:
10

3-rasm


D:\rabinM\rabinM\Release\rabinM.exe
Tublikka tekshiriluvchi n - toq sonni kiriting:
123426017006182806728593424683999798008235734137469123231828679
Raundlar soni t ni kiriting:
10
temp=0
n1=617130085030914033642967123419998990041178670687345616159143 39
temp=1
s=1
n1=617130085030914033642967123419998990041178670687345616159143 39
r=617130085030914033642967123419998990041178670687345616159143 39
Tasodifiy a son tanlang:
a=17059371837913782990360073744820693918266943014740595392979120
y=123426017006182806728593424683999798008235734137469123231828678
Tasodifiy a son tanlang:
a=17059371837913782990360073744820693918266943014740595392979120
y=123426017006182806728593424683999798008235734137469123231828678
Tasodifiy a son tanlang:
a=17059371837913782990360073744820693918266943014740595392979120
y=123426017006182806728593424683999798008235734137469123231828678
Tasodifiy a son tanlang:
a=17059371837913782990360073744820693918266943014740595392979120
y=123426017006182806728593424683999798008235734137469123231828678
Tasodifiy a son tanlang:

4-rasm




5-rasm

**Xulosada,** Rabin–Miller algoritmining takomillashtirilgan ko‘rinishi asosida kriptobardoshli kalit generatsiyasini amalga oshirish algoritmi ishlab chiqildi. Ushbu algoritm orqali tublikka sinashda murakkab sonlarni aniqlash samaradorligi oshdi, shuningdek "soxta guvohlar" soni kamaytirildi. Rekursiv funksiyalar asosida ishlovchi algoritm C# dasturlash tilida yozilib, MPFR/MPIR kutubxonasi asosida katta sonlar bilan ishlash imkoniyatiga ega bo‘ldi. Tadqiqot natijalari yangi algoritmning axborot xavfsizligi sohasida yuqori darajada qo‘llanilishi mumkinligini ko‘rsatmoqda.

## Foydalanilgan adabiyotlar ro’yxati

1. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Osnovы kriptografii. Uchebnoe posobie/ Izd.:Gelios ARV, 2001. – 480 s.

2. Akbarov D.Ye., Xasanov P. F., Xasanov X. P., Axmedova O. P. “Kriptografiyaning matematik asoslari” – Toshkent, 2010 – 210 bet.

3. ISO/IEC 11770 -1. “Key management – Introduction”.

4. ISO/IEC 11770 -2. “Key management – Symmetric techniques”.

5. ISO/IEC 11770 -3. “Key management – Asymmetric techniques”.

6. Menezes A., van Oorschot R., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. – 780 rr.

7. Moldovyan A.A., Moldovyan N.A., Guts N.D., Izotov B.V. Kriptografiya. Skorostnыe shifrы. Sankt – Peterburg «BXV-Peterburg» 2002.

8. Bryus Shnayer. Prikladnaya kriptografiya. Protokolы, algoritmы, isxodnыe tekstы na yazыke SI – Moskva: TRIUMF, 2002.

9. Akbarov D.Ye. «Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo’llanilishi» - T.: «O’zbekiston markasi», 2009. - 424 b.