Mundarija

[**Kirish 3**](#_Toc199002424)

[**I.bob. Pseudo tasodifiy ketma-ketlik generatorlarining nazariy asoslarini o’rganish 6**](#_Toc199002425)

[**1.1. Tasodifiy sonlar va ularning axborot xavfsizligidagi o‘rni 6**](#_Toc199002426)

[**1.2. Pseudo tasodifiy ketma-ketlik generatorlari 7**](#_Toc199002427)

[**II.bob. Dasturiy vositalarni o’rnatish va kerakli qurilmalarni sozlash 9**](#_Toc199002428)

[**2.1. Dasturiy vositalarni o‘rnatish va sozlash 9**](#_Toc199002429)

[**2.2. Zaruriy qurilmalar va ularning xususiyatlari. Qurilmalarni ulash 10**](#_Toc199002430)

[**III.bob. Qurilma orqali Pseudo tasodifiy sonlarni hosil qilish 12**](#_Toc199002431)

[**3.1. Elementar Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish 12**](#_Toc199002432)

[**3.2. Murakkab Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish 13**](#_Toc199002433)

[**3.3. Siljitish registrlari orqali tasodifiy sonlar hosil qilish 15**](#_Toc199002434)

[**3.4. Pseudo tasodifiy ketma-ketlik generatorlarini umumiy tahlil qilish va samaradorligini oshirish bo’yicha takliflar ishlab chiqish 17**](#_Toc199002435)

[**Xulosa 19**](#_Toc199002436)

[**Foydalanilgan adabiyotlar 20**](#_Toc199002437)

# Kirish

Bugungi kunda axborot texnologiyalarining jadal rivojlanishi dunyoning har bir burchagiga o‘z ta’sirini ko‘rsatmoqda. Bu rivojlanish nafaqat kundalik hayotimizni, balki butun iqtisodiy, siyosiy va ijtimoiy tuzilmalarga ham bevosita ta’sir o‘tkazmoqda. Axborot texnologiyalarining turli sohalarda keng qo‘llanilishi ayniqsa, axborot xavfsizligini ta’minlash uchun zarur bo‘lgan kriptografik usullarni yanada dolzarb masalaga aylantirdi. Kriptografiya nafaqat shaxsiy ma’lumotlar, balki davlat va tijorat sirlarini himoya qilishda ham asosiy vosita bo‘lib xizmat qilmoqda. Hozirgi kunda sun’iy intellekt, blokcheyn texnologiyasi va boshqa ilg‘or tizimlar kriptografiya yordamida yanada xavfsiz va ishonchli tizimlarni yaratish imkonini bermoqda. Shu bilan birga, axborot xavfsizligini ta’minlash bo‘yicha bilim va ko’nikmalarga ega bo’lish faqatgina xavfsizlik sohasi mutaxassislari uchun emas, balki har bir fuqaro uchun ham zarur ekani kundek ravshan.

Yurtimizda kriptografik texnologiyalar va axborot xavfsizligi sohasi ham jadal rivojlanmoqda. Buning natijasida zamonaviy texnologiyalarga bo‘lgan talab ortmoqda va yoshlar ushbu sohada chuqur bilim olishga qiziqish bildirmoqda. Ayniqsa, kriptografiya sohasidagi talablarga javob beradigan ilg‘or texnologiyalarni o‘rganish va ishlab chiqish bugungi kunning eng muhim vazifalaridan biridir. Bu o‘z navbatida yoshlar uchun katta imkoniyatlar yaratmoqda. Talabalar, dasturchilar va mutaxassislar orasida axborot xavfsizligi, kompyuter tarmoqlari va kriptografiya sohalaridagi bilimlarni egallash ommalashmoqda. “Axborotni himoyalashning kriptografik usullari” fani soha uchun kerakli bo’lgan barcha boshlang’ich bilimlarni qamrab oladi va o’rganuvchilarga juda katta yordam beradi.

O’rgangan nazariy bilimlarimizni mustahkamlash, amaliyotda qo’llash hamda kriptografiya sohasiga oid zamonaviy qurilmalar yasashni o’rganish uchun ushbu fandan kurs ishi uchun “Pseudo tasodifiy ketma-ketlik generatorlari” mavzusini tanladik. Kriptografiya tizimlarida xavfsizlikni ta’minlash uchun ko‘plab vositalar mavjud, ulardan biri Pseudo tasodifiy ketma-ketlik generatorlari hisoblanadi. Ushbu generatorlar tasodifiy sonlar yaratishda muhim ahamiyatga ega bo‘lib, ular maxfiy kalitlarni yaratish, ma’lumotlarni shifrlash va autentifikatsiya tizimlarida keng qo‘llaniladi. Pseudo tasodifiy ketma-ketlik generatorlari o‘zining ishlash prinsipi bo‘yicha, to‘liq tasodifiy sonlarni yaratishdan farq qiladi, chunki ular ma’lum bir algoritmga asoslangan bo‘lib, natijalar faqat belgilangan boshlang‘ich shartlarga bog‘liq bo‘ladi.

Amaliyotda Pseudo tasodifiy ketma-ketlik generatorlari kriptografik kalitlarni yaratishda, xavfsiz tizimlarda ma’lumotlar almashinuvi jarayonida, autentifikatsiya qilish va ma’lumotlarning yaxlitligini tekshirishda muhim o‘rin tutadi. Shu sababli, Pseudo tasodifiy ketma-ketlik generatorlarining samaradorligini, ularning xavfsizligini va tasodifiylik darajasini yaxshilash uchun ilmiy izlanishlar olib borish zarur.

Ushbu kurs ishida Pseudo tasodifiy ketma-ketlik generatorlarining asosiy ishlash prinsiplari, turlari, ularning kriptografiya va boshqa xavfsizlik tizimlaridagi o‘rni va ahamiyati tahlil qilinadi. Shuningdek, Pseudo tasodifiy ketma-ketlik generatorlarining xavfsizlikka ta’sirini baholash, ularning samaradorligini oshirish bo‘yicha takliflar ishlab chiqish ham kurs ishining muhim qismini tashkil etadi.

Kurs ishini bajarish uchun quyidagi vazifalar belgilandi:

1. Pseudo tasodifiy ketma-ketlik generatorlarining nazariy asoslarini o’rganish.
2. Dasturiy vositalarni o’rnatish va kerakli qurilmalarni sozlash.
3. Qurilma orqali Pseudo tasodifiy sonlarni hosil qilish:

* Elementar Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish.
* Murakkab Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish.
* Siljitish registrlari orqali tasodifiy sonlar hosil qilish.
* Pseudo tasodifiy ketma-ketlik generatorlarini umumiy tahlil qilish va samaradorligini oshirish bo’yicha takliflar ishlab chiqish.

1. Kurs ishining amaliyotda qo‘llanilishi va afzalliklari haqida umumiy xulosa chiqarish.

# I.bob. Pseudo tasodifiy ketma-ketlik generatorlarining nazariy asoslarini o’rganish

## 1.1. Tasodifiy sonlar va ularning axborot xavfsizligidagi o‘rni

Axborot xavfsizligi tizimlarida ko‘plab kriptografik operatsiyalar tasodifiylikka asoslanadi. Shifrlash kalitlari, sessiya kalitlari, autentifikatsiya tokenlari, raqamli imzolar va boshqa ko‘plab himoya usullarida tasodifiy sonlar muhim rol o‘ynaydi. Shuning uchun, tasodifiy sonlar generatorlarining ishonchliligi va sifati kriptografik tizimning umumiy xavfsizligiga bevosita ta’sir ko‘rsatadi.

Tasodifiy sonlar – bu oldindan aniq bashorat qilib bo‘lmaydigan sonlardir. Ular kompyuter tizimlarida quyidagi ikki asosiy yo’l orqali hosil qilinadi:

**Haqiqiy (fizik) tasodifiy sonlar.** Bu sonlar tabiatdagi noaniq va nazorat qilib bo‘lmaydigan fizik hodisalarga asoslanadi. Ularda hech qanday algoritm ishlatilmaydi – ya’ni ular deterministik emas. Bunday hodisalar doimiy ravishda o‘zgarib turadi va inson tomonidan nazorat qilib bo‘lmaydi.

Fizik manbalar:

* Termal shovqin (elektron qurilmalardagi issiqlik tebranishlari).
* Atmosferadagi shovqinlar.
* Radioaktiv parchalanish (Geiger hisoblagichi yordamida).
* Lazer, foton yoki kvant effektlari.

Afzalliklari:

* Haqiqiy tasodifiylikka ega.
* Oldindan bashorat qilib bo‘lmaydi.

Kamchiliklari:

* Maxsus qurilmalar talab qilinadi.
* Sekin ishlaydi (odatda real vaqt rejimida yig‘iladi).
* Dasturiy ta’minotda bevosita amalga oshirish mushkul.

Asosan yuqori darajadagi kriptografik tizimlar, harbiy va ilmiy tajribalarda qo’llaniladi va juda ham ijobiy natijalar beradi.

**Pseudo tasodifiy sonlar.** Bu turdagi sonlar algoritmik asosda ishlab chiqiladigan sonlar bo‘lib, ularning tashqi ko‘rinishi tasodifiy bo‘lsa-da, aslida aniq formulaga asoslanadi. Bu sonlar kompyuter dasturi orqali yaratiladi va bir xil boshlang‘ich qiymatdan har doim bir xil natija hosil qiladi.

Ishlash prinsipi:

* Dastlabki qiymat olinadi.
* Maxsus matematik formula orqali keyingi qiymatlar hosil qilinadi.
* Har bir keyingi son avvalgi asosida hisoblanadi.

Afzalliklari:

* Juda tez ishlaydi.
* Dasturiy usulda osongina qo‘llaniladi.
* Har xil statistik testlardan o‘tgan algoritmlar mavjud.

Kamchiliklari:

* Deterministik bo‘lgani uchun maxfiylik pastroq.
* Agar boshlang’ich qiymat ma’lum bo‘lsa, butun ketma-ketlikni tiklash mumkin.
* Ba’zi oddiy algoritmlar bashorat qilishga oson bo‘ladi.

Kompyuter o‘yinlari, simulyatsiyalar, statistik modellash hamda umumiy dasturlash sohalarida qo’llaniladi, ba’zida shifrlashda ham ishlatilishi mumkin.

## 1.2. Pseudo tasodifiy ketma-ketlik generatorlari

**Pseudo tasodifiy ketma-ketlik generatorlari** (PRNG – Pseudo Random Number Generator) – bu deterministik algoritmlar bo‘lib, ular boshlang‘ich qiymat asosida "tasodifiy ko‘rinishga ega" sonlar ketma-ketligini hosil qiladi.

PRNG’larning asosiy xususiyatlari quyidagilardan iborat:

* Takrorlanuvchanlik: Bir xil boshlang‘ich qiymat bilan boshlansa, har safar bir xil ketma-ketlik hosil bo‘ladi.
* Tezkorlik: Juda katta hajmdagi sonlarni tezda hosil qilishi mumkin.
* Statistik tasodifiylik: Hosil qilingan sonlar statistik testlardan o‘tganda, tasodifiyga juda yaqin ko‘rinadi.
* Deterministiklik: Agar dushman boshlang‘ich qiymatni bilsa, butun ketma-ketlikni tiklay oladi.

PRNG algoritmlari odatda quyidagi ko‘rinishda bo‘ladi:

**x₀ = boshlang’ich qiymat**

**x₁ = f(x₀)**

**x₂ = f(x₁)**

**...**

**xₙ = f(xₙ₋₁)**

Bu yerda f() – deterministik funksiya. Har bir yangi qiymat avvalgisidan hosil qilinadi. Agar PRNG sodda funksiyalar orqali generatsiya qilinadigan bo‘lsa, kriptografik tizimning barcha komponentlari xavf ostida qoladi. Masalan:

* Kalitlarni oldindan taxmin qilish mumkin bo‘ladi.
* Autentifikatsiya tokenlari qalbakilashtiriladi.
* Shifrlangan ma’lumotlar ochilishi mumkin.

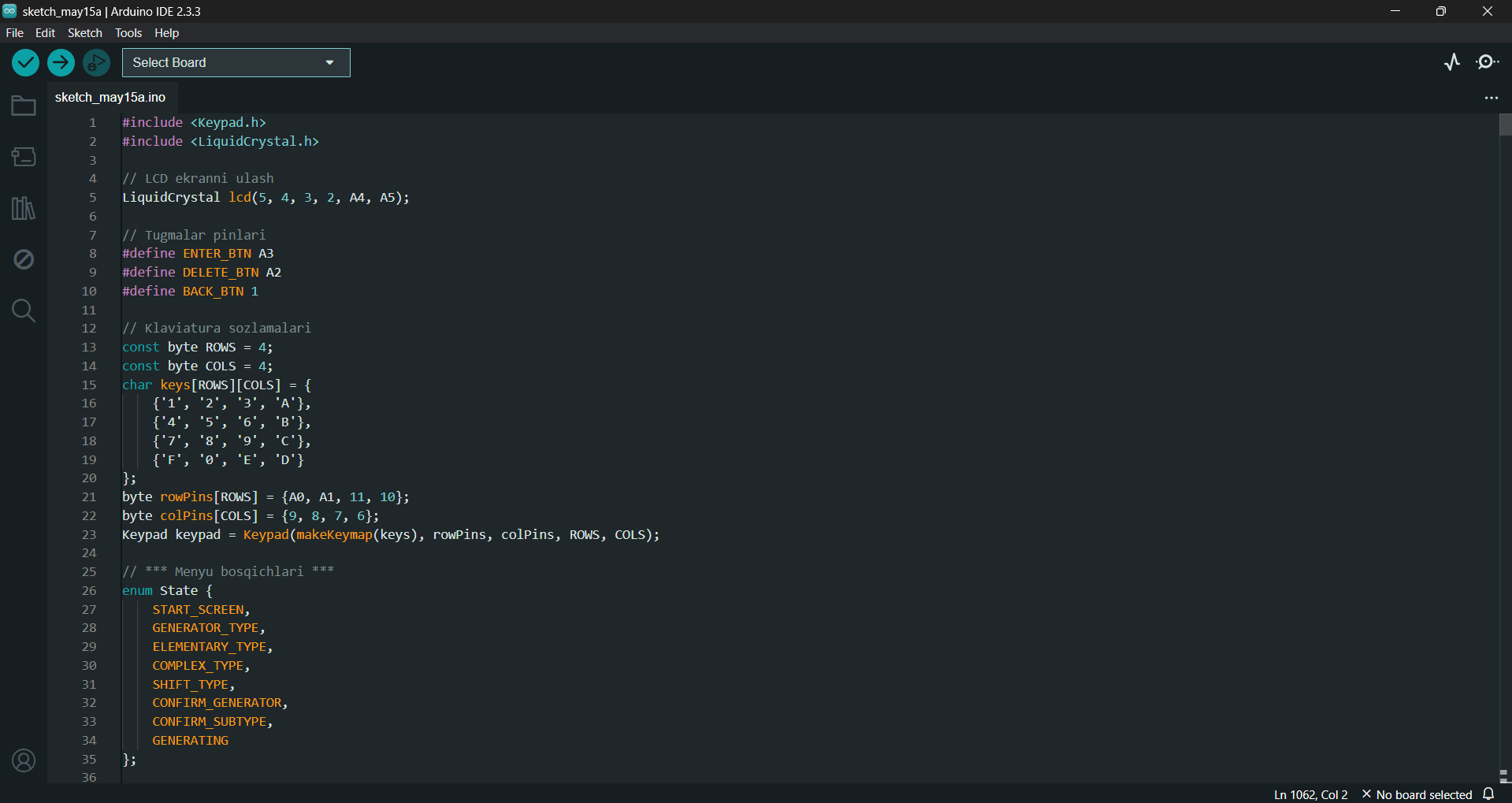
Shuning uchun PRNG tanlashda, tizim talablariga qarab, murakkab yoki kriptografik PRNG ishlatiladi. Keyingi bo’limlarda ularning turlari bilan batafsil tanishib chiqamiz.

# II.bob. Dasturiy vositalarni o’rnatish va kerakli qurilmalarni sozlash

## 2.1. Dasturiy vositalarni o‘rnatish va sozlash

Pseudo tasodifiy ketma-ketlik generatorlarini qurishda dasturiy vositalar va qurilmalarning o‘zaro uyg‘unligi muhim ahamiyat ega. Loyihani muvaffaqiyatli amalga oshirish uchun avvalo kerakli muhitni yaratish, kerakli dasturlarni o‘rnatish va qurilmalarni sozlash talab etiladi. Quyida loyiha uchun zarur bo‘lgan texnik vositalar, ularning o‘rnatilishi va moslashtirish bosqichlari bilan tanishamiz.

Arduino IDE (2.1.1-rasm) — bu Arduino mikrokontrollerlari uchun dasturlash muhiti bo‘lib, generator kodini yozish, tahrirlash va qurilmaga yuklash imkonini beradi.

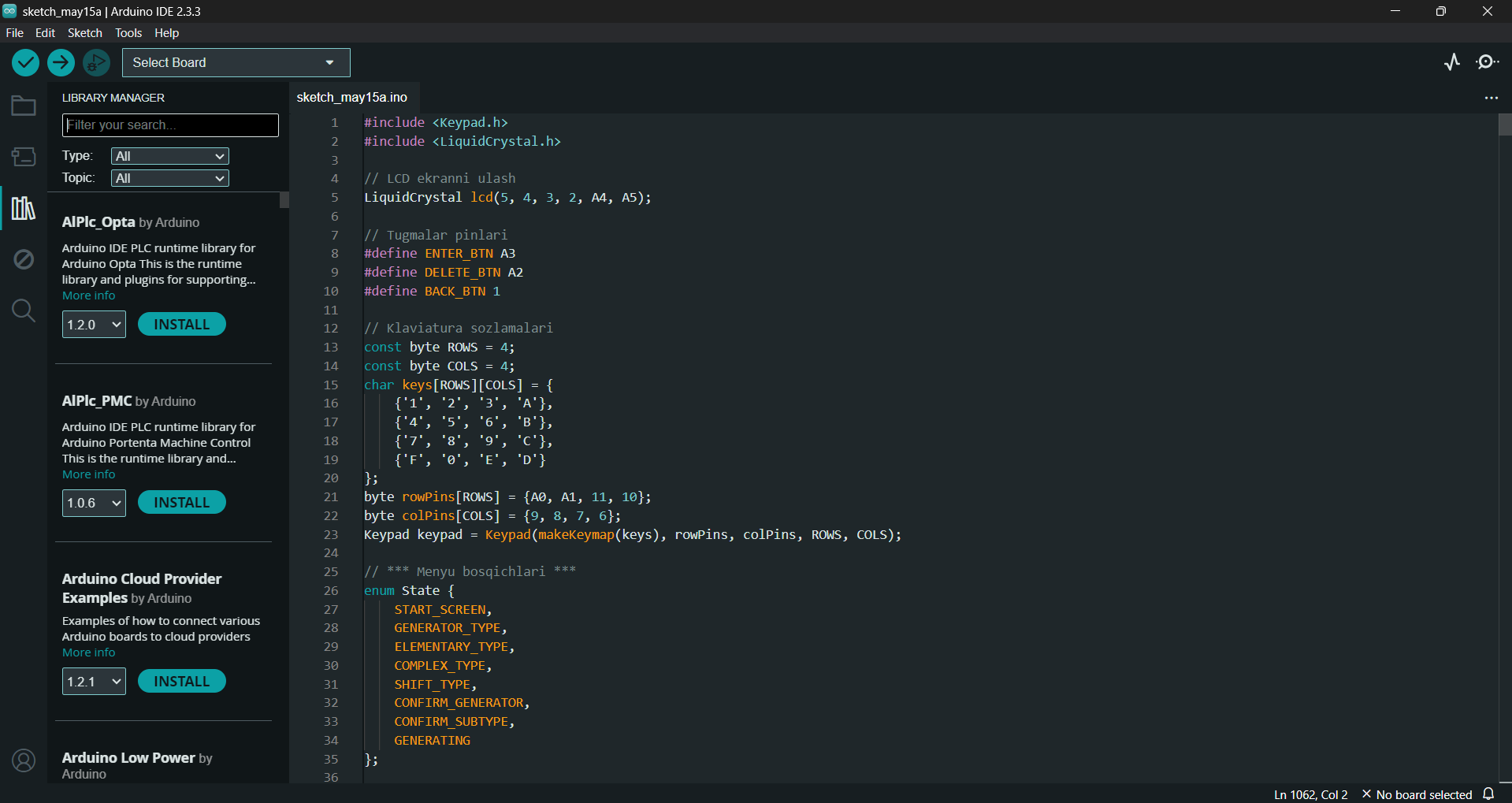


2.1.1-rasm. Arduino IDE dasturlash muhiti.

O‘rnatish bosqichlari:

1. Arduino rasmiy saytiga kiriladi.
2. Operatsion tizimga mos versiya yuklab olinadi (Windows/Linux/Mac).
3. Dastur o‘rnatiladi va Arduino Uno drayverlari avtomatik tarzda o‘rnatiladi.
4. IDE ishga tushirilgach, “Tools” menyusidan Board: Arduino Uno va Port: COMx (mos port) tanlanadi.

Arduino kutubxonalari (2.1.2-rasm). LiquidCrystal – LCD display bilan ishlash uchun kutubxona. Keypad – 4x4 o’lchamdagi klaviatura bilan ishlash uchun kutubxona. Arduino IDE’da Sketch > Include Library > <Kutubxona nomi> orqali o’rnatiladi.



2.1.2-rasm. Arduino kutubxonalarini o’rnatish.

## 2.2. Zaruriy qurilmalar va ularning xususiyatlari. Qurilmalarni ulash

Loyihani fizik jihatdan amalga oshirish uchun quyidagi qurilmalar tanlandi:

1. Arduino Uno – Ochiq kodli mikrokontroller platasidir. PRNG ishlashi uchun markaziy platforma sifatida ishlatiladi.
2. LCD displey (16x2) – Tasodifiy sonlar va menyu interfeysini ko‘rsatadi.
3. Keypad (4x4) – Foydalanuvchi tomonidan raqamlar yoki buyruqlar kiritish uchun qo‘llaniladi.
4. Pushbutton tugmalar – Foydalanuvchi bilan oddiy aloqa vositasi. “Enter”, “Delete” va “Back” tugmalari bilan boshqariladi.
5. Breadboard va simlar – Elektr ulanishlarini amalga oshirish uchun.
6. USB kabel – Arduino-ni kompyuterga ulash uchun.

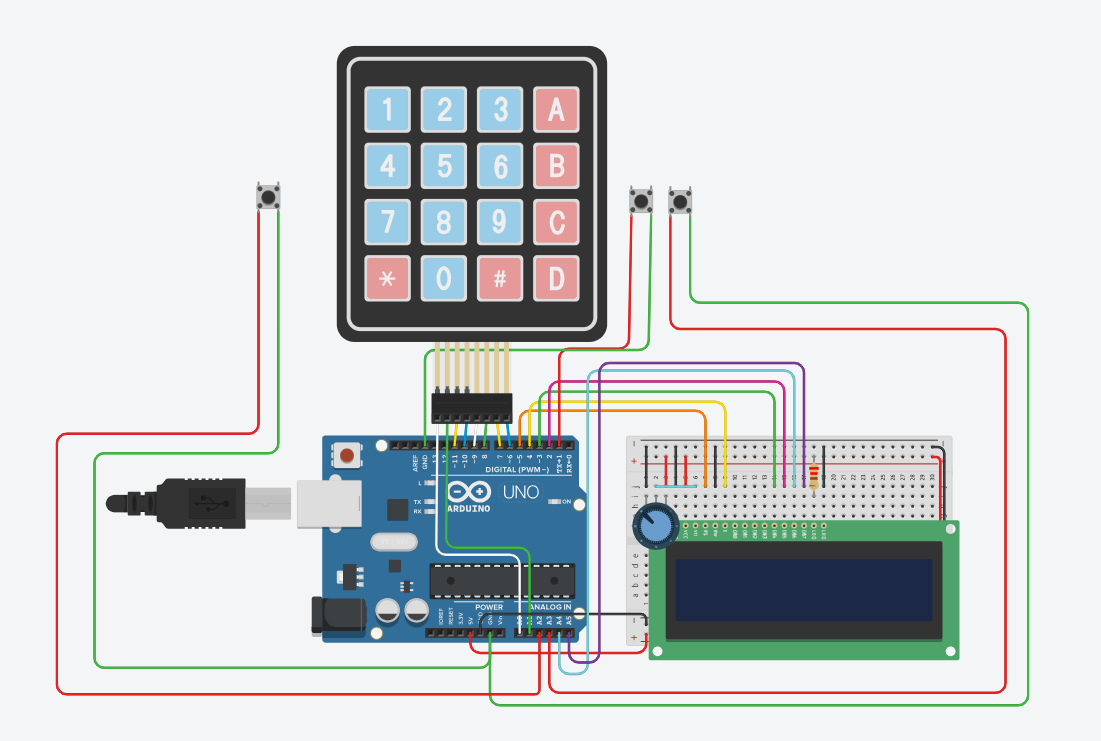
Quyida sxema va ulanish tartibi keltirilgan:

* LCD displey: RS, E, D4–D7 pinlari Arduino pinlariga ulanadi (masalan: 12, 11, 5, 4, 3, 2).
* Tugmalar: A3 (Enter), A2 (Delete), D1 (Back) pinlariga ulanadi.
* GND va VCC mos ravishda 5V va GND pinlariga ulanadi.

Tugmalarni tortish rejimi (Pull-down):

* Har bir tugma bir uchi orqali GND bilan, ikkinchi uchi esa Arduino piniga ulanadi.
* Dasturiy jihatdan pinMode(pin, INPUT); orqali sozlanadi.

Pseudo tasodifiy ketma-ketlik generatorlarini qurish uchun kerakli qurilmalarning umumiy sxemasi (2.2.1-rasm) quyidagi ko’rinishda bo’ladi:



2.2.1-rasm. Qurilmalarning umumiy sxemasi.

# III.bob. Qurilma orqali Pseudo tasodifiy sonlarni hosil qilish

## 3.1. Elementar Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish

Elementar Pseudo tasodifiy ketma-ketlik generatorlari (PRNG) eng oddiy deterministik algoritmlardan foydalangan holda, ko‘rinishda tasodifiyga o‘xshash sonlar ketma-ketligini hosil qiladi. Bunday generatorlar matematik formulalarga asoslanadi va boshlang‘ich qiymatga bog‘liq holda takrorlanadigan sonlar ketma-ketligini hosil qiladi.

Eng ko‘p qo‘llaniladigan elementar usullardan biri bu chiziqli funskiya orqali ishlaydigan generator hisoblanadi. U quyidagi formula asosida ishlaydi:

Xn+1​=(a \* Xn​ + c) mod N

Bu yerda:

* Xn​ – n-chi bosqichdagi qiymat (boshlang‘ich qiymat – X0​),
* a – ko‘paytiruvchi (multiplier),
* c – qo‘shiluvchi (increment),
* N – modul (modulus),
* Xn+1​ – keyingi qiymat.

Ushbu formuladan foydalangan holda oddiy tasodifiy ko‘rinishga ega sonlar ketma-ketligi olinadi. Nochiziqli formula orqali ham generator hosil qilinadi. Quyida nochiziqli formulani ko’rishimiz mumkin:

Xn+1​=(d \* Xn \* Xn + a \* Xn ​+ c) mod N

Bu yerda:

* Xn​ – n-chi bosqichdagi qiymat (boshlang‘ich qiymat – X0​),
* d, a – ko‘paytiruvchi (multiplier, d ≠ 0),
* c – qo‘shiluvchi (increment),
* N – modul (modulus),
* Xn+1​ – keyingi qiymat.

Ushbu metodlarning kamchiliklari:

* Takrorlanuvchanlik – Agar boshlang’ich qiymat bir xil bo‘lsa, har doim bir xil ketma-ketlik hosil bo‘ladi.
* Past entropiya – Sonlar o‘rtasidagi bog‘liqlik yuqori bo‘lishi mumkin, ko’pincha sikl tushib qolish holati kuzatiladi.
* Kriptografik jihatdan zaiflik – Kriptografik masalalarda himoya darajasi past hisoblanadi.

Shunga qaramay, elementar generatorlardan oddiy testlar, o‘yinlar yoki tasodifiy sonlar kerak bo‘lgan nisbatan xavfsizlik darajasi past bo‘lgan tizimlarda foydalanish mumkin.

## 3.2. Murakkab Pseudo tasodifiy ketma-ketlik generatorlari orqali tasodifiy sonlar hosil qilish

Murakkab Pseudo tasodifiy ketma-ketlik generatorlari (PRNG) oddiy (elementar) generatorlarga nisbatan xavfsizroq va murakkabroq algoritmlarga asoslanadi. Ular kriptografik masalalarda foydalanish uchun mo‘ljallangan bo‘lib, tasodifiylik darajasi yuqori, oldindan aytib bo‘lmaydigan ketma-ketliklar hosil qilish imkonini beradi. Murakkab PRNG’larning asosiy xususiyatlari:

* Katta davriylik: Ketma-ketlikning davri juda ham katta, siklga tushishi qiyin.
* Yuqori entropiya: Har bir yangi son avvalgilari bilan bog‘liq emasdek ko‘rinadi.
* Kriptografik barqarorlik: Tashqi kuzatuvchi uchun ketma-ketlikni oldindan aytish deyarli imkonsiz.
* Kirish holatiga sezgirlik: Boshlang‘ich holatdagi kichik o‘zgarish ham butun ketma-ketlikni o‘zgartiradi.

1. **RSA asosidagi Pseudo tasodifiy ketma-ketlik generatori.** Ushbu generator yetarlicha katta sonni tub ko’paytuvchilarga ajratish, ya’ni faktorizatsiya muammosiga asoslangan. Shuning uchun generatsiya jarayonida RSA algoritmidan foydalaniladi:

N = p \* q ϕ(N) = (p – 1) \* (q – 1)

Xn+1 = (Xn ^ e) mod N

Bu yerda:

* p, q – yetarlicha katta tub sonlar,
* e – ixtiyoriy son, shart (e, ϕ(N)) ≡ 1,
* Xn​ – n-chi bosqichdagi qiymat (boshlang‘ich qiymat – X0​),
* N – modul (modulus),
* Xn+1​ – keyingi qiymat.

Har safar X dan oxirgi bir bit ajratib olinadi va kalit hosil qilinadi.

Afzalliklari:

* Bir tomonlama funksiya sifatida RSA matematik jihatdan murakkab.
* Teskari hisoblash (masalan, boshlang‘ich qiymatni aniqlash) juda qiyin.

1. **Blum-Blum-Shub (BBS) generatori.** BBS generatori RSA generatoriga juda ham o’xshash, faqatgina boshlang’ich qiymatni kiritishda biroz farqlanadi. X qiymat kiritiladi va shu qiymat orqali X0 hosil qilib olinadi. Bundan keyingi jarayonlar RSA generatori bilan bir xil tartibda amalga oshiriladi.

N = p \* q ϕ(N) = (p – 1) \* (q – 1) X0=X2 mod N

Xn+1 = (Xn ^ e) mod N

Bu yerda:

* X – kiritiladigan boshlang’ich qiymat (X0 shu qiymat asosida hisoblanadi),
* p, q – yetarlicha katta tub sonlar,
* e – ixtiyoriy son, shart (e, ϕ(N)) ≡ 1,
* Xn​ – n-chi bosqichdagi qiymat (boshlang‘ich qiymat – X0​),
* N – modul (modulus),
* Xn+1​ – keyingi qiymat.

Bu generatorda ham RSA kabi X dan oxirgi bir bit ajratib olinadi va kalit hosil qilinadi.

1. **Blyum-Mikali generatori.** Ushbu generator diskret lagorifm muammosiga asoslangan bo’lib, generatsiya jarayoni quyidagicha amalga oshiriladi:

Xn+1 = mod p

Bu yerda:

* p – yetarlicha katta tub son,
* g – p modul bo‘yicha asos, shart g < p va (p, g) ≡ 1,
* Xn​ – n-chi bosqichdagi qiymat (boshlang‘ich qiymat – X0​).

Kalit hosil qilish jarayoni yuqoridagi generatorlardan farq qiladi. Hosil bo‘lgan X soni quyidagi shart asosida tekshiriladi:

Xn+1 <

Agar shart bajarilsa, kalitga 1 yoziladi, aks holda esa 0 yoziladi. Shu tariqa har bir qadamda kalitga bitta bit qo‘shib boriladi.

## 3.3. Siljitish registrlari orqali tasodifiy sonlar hosil qilish

Siljitish registrlari asosidagi Pseudo tasodifiy ketma-ketlik generatorlari (Shift Register-based PRNG) – bu raqamli tizimlarda keng qo‘llaniladigan, tezkor va apparat darajasida amalga oshiriladigan generatorlardir. Ular o’zaro bog‘langan registrlar orqali ishlaydi: har bir bosqichda registrdagi bitlar o‘zaro aralashtirilib, yangi bit hosil qilinadi va registr bo‘ylab siljitiladi.

Eng ko‘p uchraydigan turi – chiziqli qayta aloqa siljitish registrlari (Lineer Feedback Shift Register – LFSR) bo‘lib, ular XOR kabi oddiy mantiqiy amallar orqali ishlaydi. Bu generatorlar boshlang‘ich qiymat asosida takrorlanuvchi, ammo ko‘rinishda tasodifiyga o‘xshash ketma-ketliklar hosil qiladi. Tez ishlashi va kam resurs talab qilishi sababli mobil aloqa, raqamli kriptotizimlar, apparat shifrlash qurilmalari kabi joylarda keng qo‘llaniladi. A5/1 algoritmining mobil aloqa tizimlarida foydalanilgani ham bunga yaqqol misol bo’la oladi.

A5/1 oqimli shifrlash algoritmi – GSM mobil aloqasida qo‘llanilgan simli shifrlash algoritmi bo‘lib, uchta alohida chiziqli qayta aloqa siljitish registrlari (LFSR) asosida ishlaydi. A5/1 algoritmi simmetrik shifrlash algoritmi bo’lganligi uchun ochiq matn va kalit o’rtasida XOR amalini qo’llash orqali shifr matn hosil qilinadi hamda deshifrlash jarayonida ham aynan shu kalitdan foydalaniladi. Shifr matn va kalit o’rtasida yana bir marta XOR amalini qo’llash orqali ochiq matn hosil qilinadi. Quyida esa kalitni generatsiya qilish jarayoni bilan tanishib chiqamiz.

Birinchi bo’lib, 16 ta belgidan iborat boshlang’ich kalit kiritiladi. Bu belgilar o’n oltilik sanoq sistemasida bo’lgani uchun ushbu kalitni ikkilik sanoq sistemasiga o’tkazish orqali 64 bitli kalit hosil qilib olinadi. Hosil bo’lgan 64 bitli kalit uchta registrga taqsimlanadi:

X[19] Y[22] Z[23] (19 + 22 + 23 = 64)

Kalit hosil qilish uchun registrlarning oxirgi bitlari o’rtasida XOR amali bajariladi:

k = X[18] + Y[21] + Z[22]

Kalitning bir biti hosil qilib olingandan keyin siljish amali bajariladi. Oxirgi bitlar chiqib ketishi natijasida bo’shab qolgan joy siljish orqali to’ldiriladi. Registrlarning bitlari keyingi o’ringa o’tkaziladi va birinchi o’rin bo’sh qoladi. Keyingi qadamda har bir registrning birinchi o’rnidagi bitlarini o’rnini to’ldirish uchun yangi bitlar hosil qilib olinadi. Mana shu qismda e’tibor berish kerak bo’lgan bir jihat bor. Agar biror registrning barcha bitlari 0 ga aylangan bo’lsa, maxsus o’rindagi bit 1 bilan almashtiriladi va tasodifiylikka zarar yetishining oldi olinadi. Agar bu usul qo’llanilmasa, chiquvchi bitlar ketma-ketligi bir xil ko’rinishga kelib qoladi va bu xavfsizlik nuqtai nazaridan jiddiy muammo hisoblanadi. Maxsus o’rindagi bitlar:

X[8] – to’qqizinchi o’rindagi bit,

Y[10] – o’n birinchi o’rindagi bit,

Z[10] – o’n birinchi o’rindagi bit.

Quyidagi formulalar orqali har bir registrni to’ldiruvchi bitlar hosil qilinadi:

x = (x19 + x18 + x17 + x14 + 1),

y = (y22 + y21 + 1),

z = (z23 + z22 + z21 + z8 + 1).

Yuqoridagi formulalar orqali hosil qilingan bitlar mos ravishda X, Y, Z registrlarga joylanadi. Shunday qilib bizga kerakli uzunlikdagi kalitni yuqoridagi qadamlarni takrorlash orqali hosil qilishimiz mumkin.

## 3.4. Pseudo tasodifiy ketma-ketlik generatorlarini umumiy tahlil qilish va samaradorligini oshirish bo’yicha takliflar ishlab chiqish

Yuqoridagi har bir metodning o‘ziga xos afzallik va kamchiliklari mavjud. Masalan, elementar generatorlar sodda matematik formulalar ustiga qurilgan bo‘lib, juda tez ishlashi bilan ajralib turadi. Biroq, ularning xavfsizlik darajasi past bo‘lib, ayniqsa kriptografik himoya talab qilinadigan tizimlarda qo‘llash tavsiya etilmaydi. Chunki bu turdagi generatorlar ishlab chiqargan tasodifiy sonlar osonlik bilan bashorat qilinishi yoki nusxalanishi mumkin.

Murakkab generatorlar esa, murakkab matematik muammolar (masalan, tub sonlar, modul arifmetikasi) asosida ishlaydi. Bunday generatorlar maxfiylik nuqtai nazaridan yuqori xavfsizlikni ta’minlaydi, biroq ko’p resurslar talab qilishini, dasturlashdagi murakkablikni va ba’zan sekin ishlashini kamchilik sifatida ko‘rsatish mumkin. Ayniqsa, qurilmalarda tub sonlarni aniqlash va generatsiya qilish juda ko’p vaqt va resurs talab qiladi.

Siljitish registrlari (LFSR) asosidagi generatorlar esa apparat darajasida yuqori samaradorlikka ega. Ular kam resurs evaziga uzluksiz, mantiqan bog‘langan ketma-ketliklar hosil qiladi. Ushbu generatorlar, ayniqsa tezkor ishlov berish tizimlari (masalan, raqamli aloqa, test signallari, apparat kriptografiyasi) uchun qulay. Shunga qaramay, bu generatorlar ham haqiqiy tasodifiylikni ta’minlay olmaydi, chunki ular aniq algoritmik asosda ishlaydi va boshlang‘ich qiymatga bog‘liq.

Umuman olganda, Pseudo tasodifiy ketma-ketlik generatorlarining asosiy kamchiliklaridan biri – bu ularning haqiqiy tasodifiylik sonlarni emas, balki deterministik (aniq) algoritm asosida hosil qilingan qiymatlarni generatsiya qilishidir. Agar bu qiymatlarning boshlang‘ich holati yoki algoritmi oshkor bo‘lsa, bu xavfsizlik nuqtayi nazaridan jiddiy muammolarga olib kelishi mumkin. Shu bois, har bir tizim uchun maqsad va xavfsizlik darajasini inobatga olgan holda, mos Pseudo tasodifiy generator turini tanlash eng to‘g‘ri yondashuv hisoblanadi.

Pseudo tasodifiy ketma-ketlik generatorlarining samaradorligini oshirish va yuqori xavfsizlikni ta’minlash asosiy masalalardan hisoblanadi. Boshlang’ich qiymatlarga e’tiborli bo’lish hamda ularni deterministik usullar orqali hosil qilish o’rniga fizik hodisalardagi tasodifiy sonlardan foydalanish juda ham foydali bo’ladi. Bundan tashqari murakkab generatorlar asosida ishlab chiqilgan aralash (gibrid) tizimlardan ham foydalanish mumkin. Gibrid usullar orqali murakkab algoritmlar ishlab chiqish va xavfsizlik darajasini oshirish mumkin. Fizik qurilmalardan ajraluvchi signallardan boshlang’ich qiymat sifatida foydalanish ularning oshkor bo’lish ehtimolini keskin kamaytiradi va maxfiylikni oshirda yordam beradi. Shunday qilib, Pseudo tasodifiy ketma-ketlik generatorlarining samaradorligini oshirishda va xavfsizlik darajasini yaxshilashda boshlang‘ich qiymatlarga alohida e’tibor berish, murakkab va gibrid algoritmlar asosidagi tizimlar ishlab chiqish hamda fizik manbalarga asoslangan noaniqliklardan foydalanish kabi yondashuvlardan foydalanish mumkin. Bu yondashuvlar nafaqat matematik modelning barqarorligini ta’minlaydi, balki real tizimlarda qo‘llanilishi mumkin bo‘lgan ishonchli va himoyalangan yechimlar ishlab chiqishga xizmat qiladi.

# Xulosa

Biz ushbu kurs ishida Pseudo tasodifiy ketma-ketlik generatorlarining nazariy asoslarini, ularning dasturiy va apparat vositalaridagi ishlatilish mexanizmlarini, turli xil generatorlar orqali tasodifiy sonlar hosil qilish texnologiyalarini o‘rgandik. Jumladan, elementar, murakkab va siljitish registrlari asosidagi generatorlarni ko‘rib chiqdik va ularning afzallik hamda kamchiliklarini tahlil qildik. Har bir metodning amaliy samaradorligi, ishlash tezligi, xavfsizlik darajasi va resurs talablariga alohida e’tibor qaratdik. Shuningdek, kurs ishidan ko’zlangan kerakli ko’nikmalar ham hosil qilindi:

* Pseudo tasodifiy ketma-ketlik generatorlarining nazariy asoslarini o’rgandik.
* Dasturiy vositalarni o’rnatdik va kerakli qurilmalarni sozladik.
* Qurilma orqali Pseudo tasodifiy sonlarni hosil qildik.
* Kurs ishi davomida bajarilgan amaliyotlardan kerakli xulosalarni chiqardik.

Pseudo tasodifiy generatorlar yuqori aniqlikda va tezlikda ishlay olishi bilan birga, boshlang‘ich qiymatlarga bog‘liqligi sababli ba’zi xavfsizlik muammolariga duch kelishi mumkin. Shuning uchun bunday tizimlarda boshlang‘ich qiymatlarni fizik manbalardan olishni, aralash algoritmlar asosida ishlovchi gibrid tizimlardan foydalanishni taklif etdik.

Kurs ishining ahamiyati shundaki, Pseudo tasodifiy sonlar ko‘plab sohalarda – kriptografiya, simulyatsiya, o‘yinlar, signallarni qayta ishlash, sun’iy intellekt tizimlarida keng qo‘llaniladi. Ushbu kurs ishida ko‘rib chiqilgan metodlar va tahlillar, kelgusida real xavfsizlik tizimlarini loyihalashda, shuningdek, ilmiy izlanishlar olib borishda muhim ahamiyat kasb etadi.

Kurs ishini bajarish davomida duch kelgan muammo va savollarimizga kurs ishi rahbarimiz tomonidan kerakli maslahat, tavsiya va amaliy yordamlar berildi. Ushbu kurs ishi davomida olgan bilimlarimiz kelajakdagi faoliyatimizda asqotishiga ishonamiz.

# Foydalanilgan adabiyotlar

1. <https://www.arduino.cc/>
2. <https://github.com/>
3. <https://en.wikipedia.org/wiki/Linear-feedback_shift_register>
4. <https://en.wikipedia.org/wiki/Pseudorandom_number_generator>
5. <https://chatgpt.com/>
6. <https://www.tinkercad.com/>
7. <https://www.tinkercad.com/things/1n5ShPoYTZu-kriptologiya-kurs-ishi>
8. <https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/>
9. <https://youtu.be/q2XVhTWJ-Oo?feature=shared>
10. <https://youtu.be/C82JyCmtKWg?feature=shared>