Kirish

Inson hayotda duch keladigan hodisalar, jarayonlar, narsalarning aksariyati tasodifiy xususiyatga ega. Ularni yetarlicha tavsiflash, o'rganish va modellashtirish uchun deterministik usullardan foydalanishning o'zi etarli emas (ba'zi bir algoritm bilan to'liq aniqlanadi), shuning uchun tasodifiy sonlar ketma-ketligi va ularni hosil qiluvchi qurilmalar va algoritmlar (tasodifiy ketma-ketliklarning generatorlari) fanda keng qo'llaniladi. muhandislik, aloqa va axborot texnologiyalari. Axborot xavfsizligi kabi sohada tasodifiy ketma-ketliklar alohida rol o'ynaydi. Axborot xavfsizligi muammosini hal qilishning eng samarali va istiqbolli yondashuvlaridan biri bu kriptografik usullardan foydalanish bo'lib, unda tasodifiy ketma-ketlik generatorlari ko'pincha asosiy komponentlar bo'lib, asosan ularning ishonchliligini belgilaydi. Taklif etilayotgan qo'llanmada tasodifiy ketma-ketliklar, ulardan foydalanish, olish va sinovdan o'tkazish haqida asosiy ma'lumotlar keltirilgan.

Qo‘llanma 5 bo‘lim, ilova va tavsiya etilgan adabiyotlar ro‘yxatidan iborat. Har bir bo'lim o'rganilayotgan materialning o'zlashtirilishini nazorat qilish uchun savollar bilan birga keladi. Birinchi bo'limda tasodifiy sonlarni qo'llash sohalari va ularni olish usullari haqida ma'lumotlar mavjud. Ikkinchi va uchinchi bo'limlar mos ravishda haqiqiy tasodifiy va psevdo tasodifiy ketma-ketliklarning generatorlariga bag'ishlangan. Generatorning ishlashining umumiy tamoyillari ko'rib chiqiladi, ularning tasnifi, asosiy ishlab chiqarish usullari, xarakteristikalari, shuningdek, amalga oshirish misollari keltirilgan. Haqiqiy tasodifiy ketma-ketlik generatorlari uchun qayta ishlashdan keyingi jarayon muhokama qilinadi. To'rtinchi bo'lim psevdo-tasodifiy ketma-ketliklarning kriptoga chidamli generatorlarining ta'riflarini, bunday generatorlarga qo'yiladigan talablarni, ularning asosiy turlarini o'z ichiga oladi. Beshinchi bo'limda tasodifiy ketma-ketlik generatorlari sifatini tekshirishning asosiy yondashuvlari ko'rsatilgan. Eng keng tarqalgan test to'plamlari qisqacha tavsiflanadi. NIST STS statistik testlarining taniqli to'plami batafsil ko'rib chiqiladi. Ba'zi yangi sinov vositalari haqida ma'lumot beradi. Ilovada ehtimollar nazariyasi, matematik statistika va chekli maydonlar nazariyasidan kerakli materiallar mavjud.

Qo‘llanma “Axborot xavfsizligi” (10.03.01 va 10.04.01) yo‘nalishi bo‘yicha axborot xavfsizligi va xususan, axborotni himoya qilishning kriptografik usullaridan foydalanish bilan bog‘liq fanlarni o‘rganuvchi talabalar uchun mo‘ljallangan.

Qo'llanmada keltirilgan materialni ishlab chiqish ehtimollik nazariyasi asoslarini, chekli maydonlar nazariyasini bilishni, shuningdek, 5 ta shifrlash algoritmi haqida asosiy tushunchani talab qiladi. 1-3 bo'limlar tasodifiy ketma-ketliklar va ularni yaratish usullari bilan tanishtirish uchun mo'ljallangan. Ular birinchi navbatda bakalavriat talabalariga qaratilgan. 4 va 5 bo'limlardan kriptografiyaga ixtisoslashgan bakalavrlarga dars berishda foydalanish maqsadga muvofiqdir.

**1-bo'lim. Tasodifiy ketma-ketliklar. Ilovalar va ishlab chiqarish usullari**

**1.1 Tasodifiy ketma-ketliklar va ularning qo'llanilishi**

Atrofimizdagi narsalar, hodisalar va davom etayotgan jarayonlarning aksariyati tasodifiy xarakterga ega. Adekvat tavsif, o'rganish va modellashtirish uchun deterministik yondashuvlar ko'pincha etarli emas, shuning uchun turli muammolarni hal qilish uchun stokastik (ya'ni tasodifiy xarakterga ega) usullardan foydalanish tabiiydir. Shu munosabat bilan tasodifiy sonlar, bunday sonlar ketma-ketligi va ularni hosil qiluvchi generatorlar fan, texnika, aloqa, turli axborot texnologiyalari, shuningdek, kundalik hayotning ko‘p jabhalarida tobora ko‘proq foydalanilmoqda [1-13].

Tarixan kuzatishlarni tanlab olish uchun uzluksizlar o'rniga tasodifiy sonlar qo'llanila boshlandi. Tasodifiy raqamlar murakkab hisoblash masalalarini hal qilishda va hisoblash usullarini amalga oshirishda qo'llaniladi (masalan, Monte-Karlo usuli). EHMlarning rivojlanishi, bir tomondan, tasodifiy sonlardan foydalangan holda masalalar doirasini kengaytirsa, ikkinchi tomondan, ularni yaratish sifatiga yuqori talablar qo‘ydi. Vaqt o'tishi bilan tasodifiy sonlar informatika, taqsimlangan hisoblash, kriptografiya va boshqa sohalarda hal qiluvchi rol o'ynay boshladi.

Raqamlar ketma-ketligi, agar algoritmni va barcha dastlabki ma'lumotlarni bilgan holda uni takrorlashning iloji bo'lmasa, tasodifiy deb ataladi (generatorni bir xil sharoitda ikki marta ishga tushirib, biz turli xil ketma-ketliklarni olamiz). Ammo kompyuter tizimlari deterministikdir; ular qat'iy belgilangan holatlar to'plami bilan tavsiflanadi (bunday holatlar soni juda ko'p bo'lishi mumkin, lekin cheklangan). Bu ular yaratadigan ketma-ketliklar davriy va takrorlanadigan bo'lishiga olib keladi - bunday ketma-ketliklar psevdo-tasodifiy deb ataladi. Ma'lumki, davriy hamma narsa ma'lum darajada bashorat qilinadi; tasodifiy bo'lmagan. Haqiqiy tasodifiy ketma-ketliklarni olish juda mashaqqatli. Bundan tashqari, har bir jismoniy yoki axborot jarayoni ularni yaratish uchun mos emas.

Tasodifiy ketma-ketliklar inson faoliyatining turli sohalarida qo'llaniladi. Quyida tasodifiy ketma-ketliklar eng intensiv ishlatiladigan eng mashhur sohalar ro'yxati keltirilgan.

1. **Kriptografiya.** Kriptografik usullar axborot xavfsizligini ta'minlashda asosiy hisoblanadi. Kriptografiyada tasodifiy ketma-ketliklar hal qiluvchi rol o'ynaydi. Ular, xususan, ishlatiladigan shifrlash algoritmining kalitlar ketma-ketligini olish, oqim shifrlari diapazonini yaratish, shuningdek, ishga tushirish vektorlarini (blok shifrlarini) yaratish uchun ishlatiladi.
2. **Axborotni himoya qilishning boshqa sohalari.** Tasodifiy ketma-ketliklar parollar va foydalanuvchi kalitlarini shakllantirishda ajralmas hisoblanadi (yaxshi parol tasodifiy belgilarning qisqa ketma-ketligidir). Bundan tashqari, ular turli xil ma'lumotlarni himoya qilish algoritmlari natijalariga noaniqlik kiritish uchun, shuningdek, yon kanallarning oqishidan himoya qilish algoritmlari bosqichlarining davomiyligi uchun ishlatilishi mumkin. Ular autentifikatsiya qilish uchun tasodifiy so'rovlarni yaratishda va boshqa ko'plab muammolarni hal qilishda ham kerak.