

6. Generování náhodných čísel a testování generátorů

Zadání:

Tento úkol bude poněkud kreativnější charakteru. Vaším úkolem je vytvořit vlastní generátor semínka do pseudonáhodných algoritmů. Jazyk Python umí sbírat přes ovladače hardwarových zařízení různá fyzická a fyzikální data. Můžete i sbírat data z historie prohlížeče, snímání pohybu myši, vyzvání uživatele zadat náhodné úhozy do klávesnice a jiná unikátní data uživatelů.

Řešení:

Rozhodla jsem se vytvořit generátor pseudonáhodných čísel, který sbírá data pozice myši při jejím pohybu a na základě těchto pozic jsem udělala pár matematických operací, kterými pak vznikly náhodná čísla.

Kód:

Jako první jsem si vytvořila funkci, která mi vrátí pozici myši x a y. K tomu jsem použila knihovnu pyautogui. Pyautogui.position() mi najde pozici myši x a y. Pozici uloží do tuple, proto si rovnou v tomto tuple první pozici pojmenuji jako x a druhou jako y. Pozice myši závisí na rozlišení obrazovky, tudíž čísla, která z pozice myši dostaneme, jsou pouze v určitém intervalu.

Poté jsem vytvořila funkci, která mi vygenerovala náhodné číslo. V této funkci jsem první vytvořila cyklus while, který zkontroloval momentální pozici myši, pokud je pozice jiná než pozice minulá, tak jí uloží do listu pozice, jinak čeká na pohyb myši, aby se pozice změnila. Pozici myši bere vždy po 0.1 sekundě, to zařizuje knihovna time. Time.sleep() zastaví cyklus podle hodnoty v závorce, toto jsem přidala proto, aby se člověk pohybem myši stihnul dostat o trochu dál, jinak by se braly pouze pozice, které jsou těsně vedle sebe. Cyklus skončí, když máme v listu pozice 10 pozic. Toto může být v kódu jednoduše přepsáno na délku, jakou bude, kdo chtít. Dále si naimportuji náhodné číslo od 0 do 1000, toto taky může být změněno na rozsah, jaký si, kdo bude přát. Čím větší rozsah zvolím, tím bude pravděpodobnější, že budu mít vyšší čísla. A na konec cyklem for procházím list pozic, kde mezi každou pozicí provedu operaci XOR, vynásobím 10 a mezi výsledkem a náhodným číslem znovu provedu operaci XOR. Takto to bude pokračovat, dokud se neprojdou všechny dvojice v listu pozic a vrátí se nám finální náhodné číslo.

```

def generator_nahodneho_cisla():
    pozice = []
    minula_pozice = pozice_mysi()

    while True:
        momentalni_pozice = pozice_mysi()
        if momentalni_pozice != minula_pozice: #
            pozice.append(momentalni_pozice)
            minula_pozice = momentalni_pozice

        time.sleep(0.1) #Počká 0.1 sekundy než v

        if len(pozice) == 10:
            break

    #Vygeneruje náhodné číslo na základě pozice
    nahodne_cislo = random.randint(0, 10000)
    for x, y in pozice:
        nahodne_cislo ^= (x ^ y) * 10 #Provede c

    return nahodne_cislo

```

Kód už teď jen stačí použít a otestovat. Do proměnné `pocet_nahodnych_cisel` si zadám, kolik náhodných čísel budu chtít. Poznámka, čím více náhodných čísel budu chtít, tím déle budu muset pohybovat myší po obrazovce a proces může trvat pak velice dlouho. Dále si k otestování vytvořím slovník, kam budu ukládat čísla, která se mi objevila vícekrát a zároveň spočítám, kolikrát se dané číslo objevilo, proto když číslo poprvé přidám, dávám mu value 2, protože už se objevilo podruhé, poprvé bylo totiž přidáno do seznamu náhodných čísel. Při generaci 100 čísel mi vyšel výsledek zobrazen níže.

```

seznam_nahodnych_cisel = []
seznam_stejných_cisel = {}
pocet_nahodnych_cisel = 100

for i in range(pocet_nahodnych_cisel):
    nahodne_cislo = generator_nahodneho_cisla()
    if nahodne_cislo in seznam_nahodnych_cisel:
        if nahodne_cislo in seznam_stejných_cisel:
            seznam_stejných_cisel[nahodne_cislo] += 1
        else:
            seznam_stejných_cisel[nahodne_cislo] = 2
    else:
        seznam_nahodnych_cisel.append(nahodne_cislo)

print(f"Seznam náhodných čísel: {seznam_nahodnych_cisel}")
print(f"Seznam stejných náhodných čísel: {seznam_stejných_cisel}")

```

```
Seznam náhodných čísel: [2, 1839, 11885, 10593, 11297, 13370, 4156, 10294, 6045, 4305, 23254, 14699, 19336, 826, 11563, 5378, 28311, 17792, 3959, 15382, 4866, 29599, 6236, 13259, 20487, 1864, 22783, 28616, 29510, 14953, 987, 6241, 15285, 8715, 21607, 9503, 28504, 22409, 3276, 12350, 3285, 28070, 4263, 30479, 10485, 3119, 27101, 8959, 30919, 22200, 1507, 3260, 18625, 18817, 7567, 6976, 11052, 9796, 4393, 32266, 3516, 3745, 483, 5271, 8944, 2342, 10234, 23855, 7865, 5394, 21627, 10622, 4166, 28909, 10985, 29108, 27909, 12619, 31860, 24564, 1571, 13811, 6107, 17854, 175, 5834, 16040, 24624, 2123, 10075, 20497, 4664, 6278, 3156, 13290, 31821, 16138, 4836, 18253, 1605]
Seznam stejných náhodných čísel: {}
```

I když v tomto případě mi nevygenerovalo žádné číslo vícekrát, dá se předpokládat, že při generování vícero čísel by to tak bylo, právě proto, že pozice myši je určitý interval, a stejně tak je určitým intervalem číslo, které používáme ve výpočtu náhodného čísla. Ovšem tento generátor se sám o sobě nehodí ke generaci vícero náhodných čísel, a to z důvodu trvání, aby člověk vygeneroval 1000+ náhodných čísel, musel by myší hýbat opravdu dlouho.