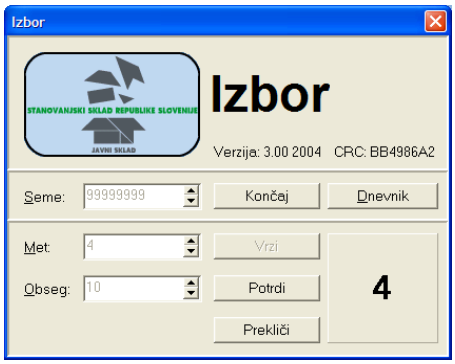
Računalniški program za naključni izbor

1. Namen

Računalniški program za naključni izbor kandidatov v okviru razpisa Stanovanjskega sklada Republike Slovenije, javnega sklada je v osnovi generator psevdonaključnih števil, ki je zasnovan tako, da je mogoče vedno preveriti in dokazati njegovo poštenost, se pravi nepristranskost in neodvisnost od trenutnih podatkov, ki so predmet naključnega izbora.



2. Funkcije programa

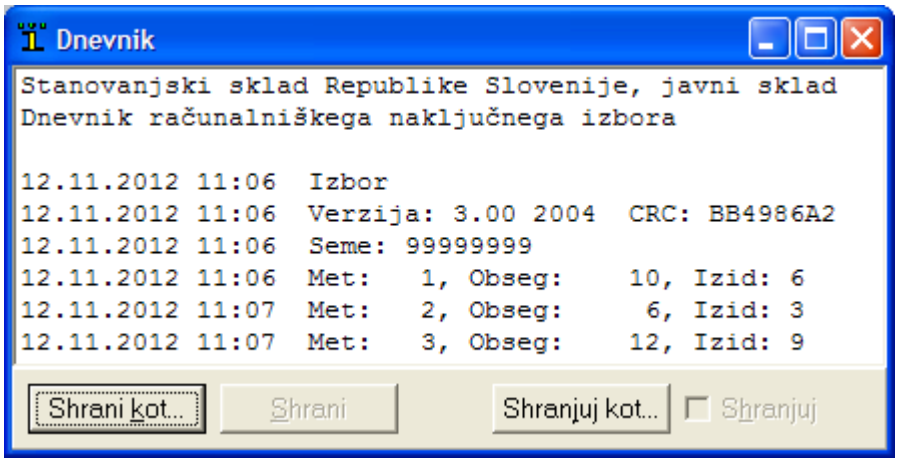
(1) Osnovna funkcija programa je generiranje zaporedja psevdonaključnih števil. Gre za zaporedja števil, katerih vrednosti se po vrsti spreminjajo, kot da bi bile rezultat slučajnih procesov, na primer meta kocke. V osnovi gre za vrednosti med 0 in 1 (0 vključno in 1 izključno), ki se v okviru programa za vsak met posebej linearno preslikajo v interval celih števil med 1 in zgornjo mejo, določeno v polju "Obseg".

(2) Osnovo za generiranje zaporedja predstavlja začetna vrednost ("seme"), ki je celo število v obsegu med 1 in 2147483647. Ista začetna vrednost vedno generira enako zaporedje števil med 0 in 1. To pomeni, da bo program pri istih začetnih vrednostih in pri istih obsegih, določenih pri vsakem metu, vedno generiral enaka zaporedja izidov. Zaporedja pri različnih začetnih vrednostih bodo različna.

(3) Program generira zaporedja po algoritmu Ran3, objavljenem v knjigi: W.H. Press, idr.: *Numerical Recipes in C: The Art of Scientific Computing*, Cambridge University Press, 1988, stran 283.

(4) Druga funkcija programa je sprotno pisanje dnevnika izidov, ki za vsak "met" vključuje podatek o datumu in času meta, zahtevani obseg in doseženi izid. Na začetku dnevnika sta izpisana tudi trenutna verzija in oznaka CRC samega programa. Dnevnik je možno shraniti na datoteko in praviloma predstavlja del zapisnika o opravljenih naključnih izborih.

(5) Oznako CRC (Cyclic Redundancy Check) izračuna sam program pred začetkom delovanja in sicer tako, da prebere lastno izvršno datoteko (Izbor.exe) in izračuna CRC po enakem algoritmu, kot ga uporablja znani program za stiskanje datotek PkZip oziroma WinZip. Vsaka sprememba izvršne datoteke z veliko verjetnostjo povzroči tudi spremembo te oznake. CRC zato predstavlja zelo zanesljiv indikator, s katerim je možno preveriti, ali je bil za naključni izbor dejansko uporabljen povsem enak program, kakršen je bil pred žrebanjem predstavljen in predan članom komisije.



3. Preverjanje programa

(1) Elementi, ki omogočajo preverjanje in dokazovanje poštenosti programa, so naslednji:

- Psevdonaključna števila so izračunana po kvalitetnem algoritmu, objavljenem v računalniški strokovni literaturi.
- Pred žrebanjem se program na mediju, ki onemogoča dodatne popravke, preda članom komisije, ki ga lahko naknadno preverjajo.
- Delovanje programa je ponovljivo, saj zagotavlja enaka zaporedja pri enakih začetnih pogojih, se pravi pri enaki začetni vrednosti ("seme") in enakih obsegih, ki se določajo pri vsakem metu posebej.
- S preizkusom in drugimi meritvami programa je mogoče preveriti, da različne začetne vrednosti dejansko generirajo različna zaporedja števil, ki so dejansko psevdonaključna.
- Program sproti piše dnevnik, ki ni samo dokumentacija izidov, ampak tudi dokaz, da je program dejansko deloval v skladu s tukaj zapisanimi značilnostmi.
- CRC je standardna in praktično enolična oznaka izvršne datoteke, ki onemogoča njeno naknadno zamenjavo z drugo, nepošteno.

4. Zahteve

(1) Program deluje v okolju Windows in v tem okviru nima nobenih posebnih zahtev. Programski paket sestavljata samo izvršna datoteka (Izbor.exe) in ta dokument (Izbor.doc). Namestitev paketa ni potrebna, zadošča samostojno izvajanje izvršne datoteke.

(2) Začetna vrednost ("seme") mora biti določena naključno in na način, ki izključuje možnost vplivanja na izbor te vrednosti.

5. Uporaba programa pri izboru najemnikov

(1) V konkretnem primeru dodeljevanja stanovanj na Stanovanjskem skladu Republike Slovenije, javnem skladu je postopek naslednji:

(a) Izbor najemnikov poteka pred komisijo, ki jo določi direktor SSRS.

(b) Na začetku postopka izbora najemnikov predsednik komisije neodvisno in v tajnosti določi in zapiše dvomestno število med 0 in 99. Zapisano število se upošteva kot dvomestno npr. 3 se upošteva kot 03. Prav tako neodvisno in v tajnosti dva člana komisije zapišeta trimestno število med 0 in 999. Vsako zapisano število se upošteva kot trimestno, npr. 3 se upošteva kot 003.

(c) Vodja postopka izbora prevzame vse zaprte lističe, jih med seboj premeša in ponudi enemu izmed članov komisije, da jih izbere. V vrstnem redu tega izbora se številke vnesejo kot »seme« v program. S tem je program pripravljen za uporabo v postopku izbora najemnikov.

(d) Dnevnik vseh izidov se po zaključku postopka izbora najemnikov izpiše na tiskalnik. Vsi sodelujoči pri izboru najemnikov ga podpišejo za arhiv.