Katedra informatiky

Fakulta aplikovaných věd
Západočeská univerzita
http://informatika.zcu.cz

NÁHODNÁ ČÍSLA

Generátory náhodných čísel rozlišujeme dva základní druhy. Stutečný nedeterministický generátor náhodných čísel a generátor pseudonáhodných čísel.

Ve všech programovacích jazycích jako jsou Java, C# nebo C a obecně v informatice využíváme převážně pseudonáhodné generátory.

Generátor pseudonáhodných čísel je deterministický algoritmus, který generuje posloupnost čísel. Tato posloupnost čsel by neměla být klasickými statistickými testy výpočetně rozlišitelná od náhodné. Sekvence pro graficky bezpečný musí splňovat dvě podmínky:

1. Pseudonáhodnost. Generátor musí splňovat podmínky testu následujícího bitu. Pokud vezmeme k vygenerovaných bitů, pak neexistuje žádný algoritmus, který by v polynomiálním čase spočítal bit k+1 s pravděpodobností větší než jedna polovina.

2. Dopředná bezpečnost. Generátor musí být odolný i při úniku některých nebo všech informací o jeho stavu. Zpětná rekonstrukce vygenerované sekvence nesmí být podle těchto informací možná.

Implementace v jazyce Java

```
public class Generator {
  public static Random rnd;

  public Generator(long seminko){
       rnd = new Random(seminko);
  }

  public static int generuj(int od, int do){
       return rnd.nextInt(do+1)+od;
  }

  public static int generuj(int od, int do. int kolik){
       int[] cisla = new int[kolik];
       for(int i = 0; i < kolik, i++)
              cisla[i] = rnd.nextInt(do+1)+od;
  return cisla;
  }
}
```

jedna vstupní data může po něaké době začít vykazovat periodicitu, tento problém je však minimální, protože inicializace posloupnosti by stejně měla probíhat častěji, než by se perioda stihla projevit. Vstupní data pro generátor jsou nazývána semínko a měla by být úplně/skutečně náhodná. Pro dvoje stejná inicializační data je samozřejmě generována totožná posloupnost (jsou-li vstupem algoritmu pouze tato inicializační data).

Kryptograficky bezpečný generátor pseudonáhodných čísel

Aby mohl být generátor pseudonáhodných čísel krypto-

Každý programovací jazyk nabízí funkci/třídu pro generování náhodných čísel. Tyto funkce/třídy vyžadují vždy tzv. semínko (angl. seed) pro svojí inicializaci. Takovým inicializačním semínkem bývá nejčastěji systémový čas, chceme-li ovšem bezpečnější a náhodnější generátor můžeme k tomu využít nástroje zabudované přímo v operačních systémech.

Na Windows se jedná o CryptoAPI, v GNU/Linuxu pak zase o /dev/random nebo /dev/urandom. Skutečně náhodné semínko implementované na hardwarové úrovní můžeme zístat z Intel RNG.