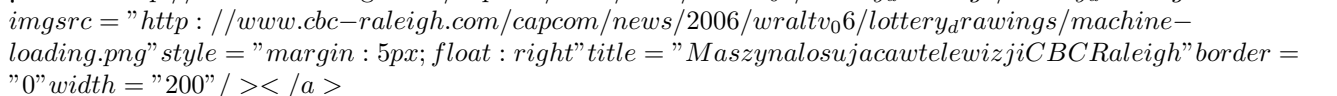


Lotto czyli komu ufa e-wyborca?

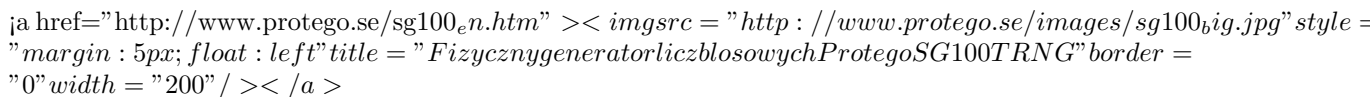
<http://ipsec.pl/komputery-wyborcze/2008/lotto-czyli-komu-ufa-e-wyborca.html>

Każdy kto oglądał kiedyś losowanie Lotto w telewizji zwrócił zapewne uwagę na sposób, w jaki losowane są poszczególne numerki. Aż się prosi by zamiast wielkich, archaicznych urządzeń wykonać prosty i zgrabny generator ciągów losowych...

```
ja href="http://www.cbc-raleigh.com/capcom/news/2006/wraltv06/lottery_drawings/lottery_drawings.html" ><
 style = "margin : 5px; float : right" title = "Maszynalosuujaca w telewizji CBC Raleigh" border =
"0" width = "200" / >< /a >
```

Współcześnie stosowane w publicznych grach losowych maszyny występują w dwóch typach, różniących się sposobem mieszania. W maszynach {grawitacyjnych kule są mieszane w obrotowym bebnie i wylatują z niego przez sterzaczki w środku wybieraka. W maszynach drugiego typu lekkie, puste w środku kule są mieszane za pomocą {sprężonego powietrza i wylatują z komory wypychane przez naciśnięcie przy otwarciu zaworu.

Na chłopski rozum stosowanie powietrznych czy grawitacyjnych maszyn losujących jest w XXI wieku niezbyt racjonalne - są głośne, żra prąd i właściwie powinny już dawno trafić do lamusa.

```
ja href="http://www.protego.se/sg100_e.n.htm" ><  style =
"margin : 5px; float : left" title = "Fizyczny generator liczb losowych Protego SG100 TRNG" border =
"0" width = "200" / >< /a >
```

Zamiast nich można by zastosować elegancki, fizyczny [ja href="http://csrc.nist.gov/groups/ST/toolkit/rng/index.html"](http://csrc.nist.gov/groups/ST/toolkit/rng/index.html) liczb losowych [i/a](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html), jakich [ja href="http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html" style="float:right" title="Dlaczego sie tego nie robi?"](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [sporodniejenarynku](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [iktoreprzechodzawszystkie](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [<ahref="http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html" style="float:right" title="Dlaczego sie tego nie robi?">](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [wymaganetestystatystyczne](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html) [.Dlaczego sie tego nie robi?"](http://csrc.nist.gov/groups/ST/toolkit/rng/rng_examples.html)

Otóż w przypadku gier losowych, w których organizator stara się przyciągnąć graczy z ich pieniędzmi do swojego systemu krytyczne jest {zaufanie co do uczciwego (tutaj: losowego) wybierania wygrywających liczb.

Czy przeciętni klienci zaufaliby grze losowej, w której wyniki są podawane przez prezentera TV z ekranu laptopa, a faktyczne losowanie odbywa się w niewielkim, czarnym pudełku? Oczywiście że nie. Oczywiście organizator mógłby publikować raporty niezależnych komisji eksperckich, potwierdzających że generator losowy jest naprawdę losowy, że przeszedł testy w NIST lub DBTI ABW i tak dalej. I cóż z tego, jeśli prawdziwość tych zapewnień może zweryfikować tylko niewielka grupa ekspertów?

Zaufanie do maszyn losujących w grach losowych wyróżnia jedno: {łatwa weryfikowalność przez wielu ludzi. Maszyny są zbudowane z plexi i przezroczyste. Zasada działania jest trywialna, intuicyjna i możliwa do zweryfikowania przez każdego człowieka, niezależnie od wykształcenia. Bardziej wyrafinowane ataki (np. manipulacja wagą kul) są eliminowane przez [ja href="http://serwis5.lotto.pl/183-41e3bd7c413d0.htm"](http://serwis5.lotto.pl/183-41e3bd7c413d0.htm) i odpowiednie procedury [i/a](http://serwis5.lotto.pl/183-41e3bd7c413d0.htm) obowiązujące komisje losujące.

Dlaczego artykuł ten trafia do działu [ja href="/podpis/e-voting-g"](/podpis/e-voting-g)

Jak widać na przykładzie Lotto, systemy {archaiczne} nadal są wykorzystywane jeśli krytyczne jest {powszechne zaufanie do systemu. Czy w przypadku wyborów powszechnych zaufanie jest czynnikiem istotnym? Chyba tak skoro budżet Lotto to ok. 2,5 mld złotych a budżet Polski to ok. 300 mld złotych.

Kilka linków, jeśli ktoś zainteresował się losowaniem {mechaniczne};

- [ja href="http://serwis5.lotto.pl/183-41e3bd7c413d0.htm"](http://serwis5.lotto.pl/183-41e3bd7c413d0.htm) i Procedura losowania w polskim Lotto [i/a](http://serwis5.lotto.pl/183-41e3bd7c413d0.htm)
- [ja href="http://serwis5.lotto.pl/183-42bbeda58647c.htm"](http://serwis5.lotto.pl/183-42bbeda58647c.htm) i Pozkłady statystyczne w polskim Lotto [i/a](http://serwis5.lotto.pl/183-42bbeda58647c.htm)
- [ja href="http://entertainment.howstuffworks.com/lottery2.htm"](http://entertainment.howstuffworks.com/lottery2.htm) i How Stuff Works: The Lotto Machines [i/a](http://entertainment.howstuffworks.com/lottery2.htm)