Temat:Generatory pseudolosowe w obliczeniach Monte Carlo i w kryptografii

Generatory liczb pseudolosowych są podstawą symulacji Monte Carlo które znalazły szerokie zastosowanie zarówno w nauce w symulacjach złożonych procesów fizycznych czy biologicznych, a także w bankowości i finansach. Równocześnie generatory liczb pseudolosowych są powszechnie używane we współczesnej kryptografii. Jednak wymagania stawiane generatorom kryptograficznym są bardziej restrykcyjne, przykładowo z wygenerowanych już próbek nie powinno się dać określić jaka będzie następna wartość próbki.
Celem pracy jest opis działania i porównanie obu typów generatorów pseudolosowych na podstawie współcześnie używanych algorytmów. Częścią pracy byłoby też implementacja i przeprowadzenie testów np. typu die-hard (Margalisa) na wybranej parze generatorów.
Praca może pójść w kierunku zarówno bardziej matematycznym jak i programistycznym, w zależności od preferencji. Projekt pozwala na pogłębienie praktycznej wiedzy w dziedzinie **kryptografii współczesnej**.

Osoby zainteresowane proszone są o kontakt mailowy: wojciech.krzemien@if.uj.edu.pl

Wymagania:
- student(-ka) 1-5 roku,
- umiejętność logicznego myślenia,
- umiejętność programowania (co najmniej podstawowa),
- silna chęć do nauki i rozwijania własnych umiejętności,
- chęć do systematycznej praca.

Mile widziane:
- doświadczenie w pracy w środowisku Linux,

Wszelkie dodatkowe informacje można uzyskać pisząc na adres: wojciech.krzemien@if.uj.edu.pl