Tema 2

Propunere 1

1. Implementați generatorul de numere pseudo-aleatoare Blum Blum Shub (BBS). În această implementare este necesar ca dimensiunea numerelor prime să fie cel puțin egală cu 256 de biți. Urmăriți pașii
2. Problema trebuie sa foloseasca un limbaj de programare la alegere (librăriile sugerate sunt Bouncy Castle în Java și GMP în C++ în Linux) si sa contina o implementare proprie (i.e., puteti utiliza librarii existente, dar trebuie sa fie si o parte semnificativa de cod care sa va apartina).
3. Tema trebuie prezentata in timpul laboratorului pana la finalul semestrului.

Link suplimentar `https://en.wikipedia.org/wiki/Blum_Blum_Shub#CITEREFBlumBlumShub1986`

Propunere 2

1. Downloadati pe Linux bateria de teste de aleatorism a celor de la NIST. Folositi link-ul `https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software`.
2. Generati un sir de numere (pseudo-)aleatoare folosind procesorul calculatorului/ laptop-ului vostru.
3. Testati aleatorismul unui sir pseudo-random folosind bateria de teste de la NIST.
4. Tema trebuie prezentata in timpul laboratorului pana la finalul semestrului.

Propunere 3

1. Alegeti 5 teste de aleatorism din bateria de teste a celor de la NIST. Acestea pot fi gasite la link-ul `https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf`.
2. Faceti o prezentare a acestora si implementati doua astfel de teste.
3. Tema trebuie prezentata in timpul laboratorului pana la finalul semestrului.

Propunere 4 Ganditi-va la un scenariu complex de utilizare al PRNG-urilor si oferiti o prezentare asupra acestuia. Este necesar ca si eu sa fiu de acord cu propunerea voastra de proiect.