Cryptography Week 2

Stream Ciphers: See Videos 2.2 – 2.7 of the Stanford Crypto course.

Pseudo-random generators – A very important concept, very easy to understand but difficult to apply.

An example: **Mersenne Twister** - http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/emt.html

https://en.wikipedia.org/wiki/Mersenne_Twister

RC4- http://crypto.stackexchange.com/questions/3643/is-there-a-way-to-make-rc4-arcfour-secure-or-is-it-completely-broken/3644#3644

LFSR - http://stackoverflow.com/questions/3735217/linear-feedback-shift-register

Try writing a basic LFSR code in python (preferred :P), upload it on pastebin etc. and pm it to me (Himanshu) or Harikrishnan for reviewing.

You can search for more modern stream ciphers, they are a bit difficult to understand (eStream variants). https://en.wikipedia.org/wiki/ESTREAM

Complete this till Friday (10/06/16) and then we'll start with Block Ciphers.