**Assignment Due Wed Oct 22**

Attached here is a serious attempt to provide you with assistance in cracking the Linear Congruential Random Number Generator given in Crypto #21.

Here is also a brief hint.

Hint: Use the solution of systems of two linear congruences and the gcd algorithm. Simultaneous linear congruences behave just like linear equations with the one difference that you can’t divide.

It is a common mistake to choose M too large, which will cause some X’s to be wrong and some to be right. If this happens, try dividing M by small primes such as 2 and 3.