

Crypto Group To DO

1. Write code that GIVEN the three equations in A, B, M that we are used to seeing, finds ALL possible solutions (A, B, M) .
2. Write code that uses all the prior program and does the following:
 - 1) INPUT: A long text T and A, B, M where A, B are rel prime, A, B are 3 digits long, and M is four digits long.
 - 2) OUTPUT: the text T encoded using the LCG $x_n = Ax_{n-1} + B \pmod{M}$.
3. Using the program above you can now generate long encoded texts.
4. Write a program that will, given a long encoded text E and a word w of length 8, does the following:
 - a) For every 8-long sequence of 2-digit numbers find all possible (A, B, M) and test if it is the real LCG. If you ever hit a real one then output the real text and stop.