

Crypto Group To DO

1. On the project website go to the slides from May 18 on Linear Cong Generators.

Read them- though you can skim the parts you already know.

For this assignment you only have to read to slide 131 titled

Thought Exp; Eve can find M (I)

2. The slides give you an example of how you can, given a set of 8 numbers that you think encode

PAKISTAN

come up with three equations in A, B, M .

Later in the sides they solve these equations; however, this assignment is not about that. (I will talk about solving them in our next meeting.)

SO do the following

- (a) Decide on a type of document you want to eventually decode (e.g., Harry Potter Novels)
 - (b) Given that type of document, come up with a word w of length $L \geq 8$ that will definitely appear (e.g., Hermione).
 - (c) Write a program that will, given a sequence of 8 2-digit numbers, assume that is how the word is coded. Assuming this, come up with equations in A, B, M . If your word has more than 8 characters than you should ignore the characters beyond the 8th. For example, if our word was
hypberbolic
only use *hyperbol*
 - (d) Note that I am only asking for the equations, not how to solve them.
 - (e) TEST your program by
 - 1) Picking A, B, M .
 - 2) Encode the word w with 8 2-digit numbers. Use your program to find the equations. Check that your A, B, M solve the equations.
3. Optional- read further in the notes