Fall 2019 CIS 3362 Homework #6
Breaking the Knapsack Cryptosystem
Check WebCourses for the due date
Please work in pairs and put both people's names on each file submitted!

A message has been encrypted using the knapsack cryptosystem. The message was created using the posted sample code, Knapsack.java. The key to breaking the code is in knowing how it was created!!!

The posted public keys are in the file publickeys.txt. The first 128 numbers are the 128 numbers of the public key set. The last number is modulo value to use.

The ciphertext to break is stored in ciphertext.txt. Each of these values is a sum of some subset of the values in the publicly posted set. Assign 1 to each value in the subset and 0 to each one not in the subset. These 128 bits can then be converted via Ascii value to 16 characters. Do this for each number to recover a text message of 17 lines, where each line has exactly 16 characters.

Good luck!!!