Fall 2019 CIS 3362 Homework #6 Grading Criteria (120 pts)

A description of the strategy that amounts to guessing a[0] or a[1] and multiplying by the inverse to obtain potential w's is worth 30 points.

Any code that looks like it's doing this and then calculating w^{-1} is worth another 15 points.

Then, if the code takes w^{-1} and multiplies it by each public set value to obtain a new set is another 15 pts.

It's another 15 pts to check if this set is super-increasing or not.

It's another 15 pts to take w^{-1}, multiply it by each ciphertext to get a target to add up to, with the super increasing set.

It's another 15 pts to convert the subset sum problem to 128 bits.

The last 15 pts is for converting those bits to bytes and obtaining the message.

Give partial credit as you deem necessary. Within this framework. If other methods were used, try to map the points as best as possible. Anyone who decodes the message and has a reasonable justification and proof of how it was done should get full credit.