1 Tutorial 3

1. Convert the super increasing sequence

$$A = \{81, 162, 322, 572, 1167, 2386, 4702, 9469, 18888, 37766, 75593, 151190, 302324, 604627, 1209249, 3926579\}$$

   into a "random" looking one by transforming it using $w = 279$ and $m = 7936729$.

   Encode the message "Sammy Cheng is cool la" by taking two characters at a time and using their ASCII bit pattern to make a selection in the "random" knapsack.

   Decrypt the encrypted message using the trapdoor (w, m, A) to recover the message.

2. For the RSA cryptosystem where $p = 8663835841$ and $q = 802360858343257$, find d for $e = 65537$. Then encrypt the message "**attack@2**" by using the concatenation of the ASCII encoding of each character in the message as a large integer. Then decrypt the cipher text using the private key to verify that you've recovered the original message.

3. Find primes p and q so that 12-bit plaintext blocks can be encrypted with RSA.

For each of these questions you may write a program to solve it. You must show (and demonstrate understanding) of all the steps needed to arrive at the answer.