MAT 2440 Assignment #4

This assignment is due on Tuesday 5/7/2019 at 10 am - at the beginning of our class period. You may submit it electronically as a pdf document or as a hard copy. Assignments late by 1 day will be penalized by 25%, 2 days late 50%, 3 days late 75% and any later they will no longer be accepted.

Please be sure this writing is your own - do NOT borrow from a friend. I want to hear your own voice, not read a copy and paste of some other source!!!

1. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the encryption function $f(p) = (p + 21) \mod 26$, and then translating the numbers back into letters. [20 points]

2. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \mod 26$. [20 points]

   (a) LO WI PBSOXN

   (b) DSWO PYB PEX

3. For the following question: Suppose that Alice and Bob have these public keys and corresponding private keys:$(n_{Alice}, e_{Alice}) = (2867, 7) = (61 \cdot 47, 7)$, $d_{Alice} = 1183$ and $(n_{Bob}, e_{Bob}) = (3127, 21) = (59 \cdot 53, 21)$, $d_{Bob} = 1149$.

   Alice wants to send to Bob the message BUY NOW so that he knows that she sent it and so that only Bob can read it. What should she send to Bob, assuming she signs the message and then **encrypts it using Bobs public key**?

   (a) First express your answer without carrying out the exponentiation calculations. [20 points]

   (b) Then, using the Python code for fast modular exponentiation found at:
   https://trinket.io/python/d2eba68dc8
   perform the calculation to get the numerical answers for the encrypted text. [20 points]

   (c) Once Bob receives Alice's encrypted message, show how he uses his decryption key d to decrypt her message. [20 points]