Math 495R Homework 11

(1) Project Euler, problem 5.
(2) Project Euler, problem 14.
(3) A *substitution cipher* is a method of encryption that replaces each letter of the alphabet with another (or possibly the same) letter of the alphabet. The key to a substitution cipher can be written as a permutation (rearrangement) of the alphabet: for instance, the key `QWERTYUIOPASDFGHJKLZXCVBNM` gives the cipher that replaces the plaintext letter `A` with the ciphertext letter `Q`, the plaintext letter `B` with the ciphertext letter `W`, and so on, so that `CAB` would be encrypted as `EQW`.

    Write functions that do the following tasks related to encrypting or decrypting substitution ciphers.

    (a) A function `permute_alphabet` that returns a random permutation of the English alphabet. (You may want to import the `random` module; see Python Essentials, chapter 2.)
    (b) A function `subst_encrypt` that takes a plaintext message and a permutation of the alphabet and returns an encrypted ciphertext message using that permutation as a substitution cipher key. The message should preserve spaces, punctuation, and any other characters that are not English letters.
    (c) A function `subst_decrypt` that takes a ciphertext message and a substitution cipher key and returns a decrypted plaintext message. Again, spacing and punctuation should be preserved if they exist in the ciphertext message. Decrypt the message

        `V: WZM EFE IZL XPI SPOO FG IZL WLOO? P: FI XHNOEG'I ALL IZPI WLOO.`

        using the key `PTXELSQZFCJODGHUVRAINKWYMB`.