CIS 3362 Homework #5: Light Coding Group - More RSA Practice

Due Date: Check Webcourses

1) A rather long ciphertext has been created using RSA. This ciphertext is attached in the file h5cipher.txt. Determine the corresponding plaintext.

2) Two separate RSA keys both use the same value of n = 418037. In particular, in one of the sets of keys, e = 234763 and in the other set of keys, e = 324977. It is known that the same message M has been encrypted using the public keys above yielding the ciphertexts 72801 and 323485, respectively. Determine integers x and y such that 234763x + 324977y = 1. Consequently, determine the original value of M without ever finding $\phi(n)$ or either value of d. (Hint: Remember what it means to raise a value to a negative exponent – first raise it to the -1 power, and then raise that result to the corresponding positive power. Furthermore, remember that raising a value to the -1 power means finding its modular inverse.) **Please show each step of your work. If you use one/edit one of the programs shown in class or write your own code, please include that in your write-up.**