CIS 3362 Homework #5: Light Coding Group Solution

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

Solution

To solve this problem, first it is necessary to convert all of numbers to mod 26. So, we will have these:

75838158 mod 26=6=f
80832869 mod 26=m
262879549 mod 26=23=w
.
.
.

So, we have following message in alphabetic:
f m w m w m f m l n I m f h l m m i k l g j t d w n n k l f f j i …

Then, a substitution cipher cracker program can be used to find plaintext. So, the plaintext is as follows:

"This is the last message you will get to break I still have some prizes so whoever is first will get these prizes although this looks really hard it is no more difficult than substitution cipher this is what we call protocol failure well good luck hopefully i put enough letters in here that you have good frequency counts oh wait I still have to tell you were the prize is this one will be buried go to the palm tree outside nearest my office from the base of the tree facing my office go two feet then dig"

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 φ(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.

Solution

For solving this problem, first we need to find x and y from equation 234763 x+324977 y=1. Extended Euclidean is used to solve this equation. You can use the posted code (http://www.cs.ucf.edu/~dmarino/ucf/cis3362/progs/ModStuff.java) to find x and y:

So, x is 82424 and y is -59543.

So, M can be calculated form following equation:

$M=M^{234763x+324977y} \bmod 418037$

So, we have:

$M^{234763x}\ M^{324977y} \equiv M \bmod 418037$
$M \equiv C1^{x} C2^{y} \bmod 418037$
$M \equiv (72801)^{82424} (323485)^{-59543} \bmod 418037$

Using the BigInteger class in Java, we can obtain M to be:

M=376512