# Alternate Crypto 4 Homework assignment

This is a problem from the spring 2021 NCL Team game.

The following was encrypted with “schoolbook” RSA, with none of the additional protections that RSA uses in real life.

Alice’s public key:

n = 1909

e = 31

Ciphertext:

1079 1189 1155 137 500 572 1659 128 137 404 42 462 42

There is a problem: n is too small!

## Hand In #1

What are the factors of 1901?

Follow the procedure in Cryptology4-Public-Key-Intro-RSA, slides 10 & 12, to recreate Alice’s public key. For n, use the value in Alice’s public key, above. For p and q, use the factors of n that you just found.

ϕ = (p-1)(q-1)

e and d are multiplicative inverses, modulo ϕ

So, d = inverse(e, ϕ)

## Hand in #2

What is d?

Now that you know n, p, q, d, and e, and n, you can decrypt the message.

Slow way: You can use the Python pow function as in slides 9 & 13 to decrypt each number. For the first number, it would be  
pow(1709, d, 1909)  
where you would insert your value of d.

Then you could look up each number in an ASCII table. Or, you could have Python do the ASCII for you with the chr function.  
chr(pow(1709, d, 1909))

Or, you could write a Python script.

## Hand In #3

What is the flag?