HOMEWORK 2

DUE 21 JANUARY 2015

SHOW ALL YOUR WORK. You are free to collaborate with your classmates. In fact, I recommend it! But keep in mind that this material will be on the quiz, so you should try to understand the solutions.

1. The message

LAKNORDTRDIEDSSDETMADAONDRUDHTEOIHYUSEJGWOOHANYTRG
BFDRRORWAETOSAHRACTDSRHIWOETISSWDSAHTVSAAEANLNMDLTA
AEHNNRASDENRBSAOLVNBAASBDLTTEYEHWREEAILSRDMPGAOEERK
LDKELAANFNSOODSTHDLYIAIRNNKIGEEAHDVNEGASLELT

has been encoded using a permutation code. Decode it.

2. Daenerys Targaryen and Jon Snow have formed an unlikely alliance. When Jon Snow receives the message

KJPXWSVHKMTMMSIVEJWWTETTQTGWJ

he knows that it was encoded using a Vigènere code with key word $WESTEROS$ and hurries to decode it. What does the message say?

3. (a) Use the affine cipher modulo

$$p = 8008808808808813$$

with key $(k_1, k_2) = (9735097, 302501)$ to encode *HELLO* after you put the word in decimal ASCII.

(b) The same key has been used to encode a message and generate the ciphertext $c = 7418224202870545$. What was the original message? The answer should be text in English, not a number.

4. Alice and Bob use the Elgamal public key system to communicate. They take each message, write it in decimal ASCII (e.g. ABC becomes 656667) ignoring spaces, and Elgamal with prime

$$p = 53542885039615245271174355315623704334284773568199$$

and primitive root $g = 3$ to encode it.

(a) Alice uses Bob's the public key

$$B = 52062272972610039279339215848234879730909313688963$$

and her ephemeral key $k = 449$ to encode the message

QUIZ ON THURSDAY. YOU READY?

and sends it to Bob. What is the ciphertext that Bob receives from Alice?

(b) Bob receives the ciphertext

$$c_1 = 514031941812662726843537672091375956858246379339 39,$$

$$c_2 = 459602772797810343098597336374874547311323013953 96$$

from Alice. He uses his private key $b = 3928749023$ to decode it. What did the original message say?

5. Alice and Bob have joined the modern world and have moved on to using RSA. They take each message, write it in decimal ASCII as in the previous exercise and then use RSA to encode it.

(a) Bob uses Alice's public key

$$N = 10195412430618261378514821214435267544817155253 73$$

and

$$e = 501589113321651433066267$$

to encode the message

DARTH VADER IS LUKE'S FATHER

and sends it to Alice. What is the ciphertext that Alice receives from Bob?

(b) Alice receives the ciphertext

$$c = 946128467512980510309544710308899482246110736 0$$

from Bob. She uses her private key

$$p = 10031782266433028661325 27 \text{ and } q = 10163111758049962356076 99$$

to decode it. What did the original message say?

6. A terrible virus has hit all the computers in the world. Or maybe they became sentient and went on strike. Who can tell? Regardless of the situation, the computing power of the whole world is diminished in such a way that humans are reduced to using only 4 digit primes. That means that in order to use Elgamal or RSA, one needs to write the text in decimal ASCII as in the previous exercises, then chop the big number representing the message into 3 digit parts, and encode each part separately.

(a) Use the public key $A = 2269$ in the public key system Elgamal with prime $p = 3823$ the primitive root $g = 3$ to encode the message

ARMAGEDDON IS NEAR

using Elgamal with ephemeral key $k = 71$. (Usually, you would use a different ephemeral key for each part of the message that you will encode, but for simplicity we will keep the same k throughout.) The answer should be a series of ciphers (c_1, c_2).

(b) A friend has used the same system (same public key, but different ephemeral keys) to encode a message and has sent you the following series of ciphers.

$$\begin{array}{cccc} (2442, 2616) & (912, 2670) & (1717, 1112) & (2323, 510) \\ (54, 3734) & (2357, 3450) & (551, 1537) & (3755, 455) \\ (476, 3255) & (358, 411) & (3116, 3479) & (1508, 1446) \end{array}$$

Recover the original message using your secret exponent $a = 1007$.

(c) Use the modulus $N = 101 \cdot 947$ and the encryption exponent $e = 701$ to encode the message

I LOVE NUMBER THEORY

with RSA.

(d) Decrypt the series of ciphers

$$93969, 34306, 23927, 50055$$

using the key from part (c).