MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #1

Problems for all

Problem 1. What is the message embedded in the following?

3rd March

Dear George,
Greetings to all at Oxford. Many thanks for your
letter and for the Summer examination package.
All Entry Forms and Fees Forms should be ready
for final despatch to the syndicate by Friday
20th or at the very latest, I'm told, by the 21st.
Admin has improved here, though there's room
for improvement still; just give us all two or three
more years and we'll really show you! Please
don't let these wretched 16+ proposals destroy
your basic O and A pattern. Certainly this
sort of change, if implemented immediately,
would bring chaos.

Problem 2. In one of Dorothy Sayers' mysteries, Lord Peter is confronted with the following message:

I thought to see the fairies in the fields, but I saw only the evil
elephants with their black backs. Woe! how that sight awed me! The
elves danced all around and about while I heard voices calling clearly.
Ah! how I tried to see–throw off the ugly cloud–but no blind eye of a
mortal was permitted to spy them. So then came minstrels, having gold
trumpets, harps and drums. These played very loudly beside me,
breaking that spell. So the dream vanished, whereat I thanked Heaven. I
shed many tears before the thin moon rose up, frail and faint as a sickle of
straw. Now though the Enchanter gnash his teeth vainly, yet shall he
return as the spring returns. Oh, wretched man! Hell gapes, Erebus now
lies open. The mouths of Death wait on thy end.

He also discovers the key to the message, which is a sequence of integers:

787656543432112343456567878878765654343211234345656787887876565443321123

(a) Decrypt the message. *[Hint: What is the largest integer value?]*
(b) If the algorithm is known but not the key, how secure is the scheme?
(c) If the key is known but not the algorithm, how secure is the scheme?

Problem 3. Find the last two digits of 123^{562}.

Date: Due Wednesday, 10 September 2008.

Problem 4. The message

`jajsymtzlmnbfqpymwtzlmymjafqqjdtkymjxmfitbtkijfymnkjfwstjanq`

was encrypted using a shift cipher. Decrypt the message. *[Hint: What are the most common letters?]*

Problem 5. Show that the following procedure defines a cryptosystem.

Choose two Caesar cipher keys k_1 and k_2. Encrypt the elements of the plaintext (written A through Z) in odd positions with k_1 and those in even position with k_2. Then reverse the order of the encrypted string.

Determine the plaintext space $\mathcal{P}$, the ciphertext space $\mathcal{C}$, and the key space $\mathcal{K}$.

Additional problems for 395A

Problem 6. Let G be a finite group, and let $k \in G$. Define the encryption function

$$\begin{aligned} E_k : G &\to G \\ g &\mapsto kg \end{aligned}$$

with $\mathcal{P} = \mathcal{C} = G$.

(a) What is the decryption function D_k? When is $E_k = D_k$?

(b) If we define $E'_k : G \to G$ by $E'_k(g) = gk$, when is $E_k = E'_k$?