Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest

Handout 3
September 18, 1997

Solutions to Problem Set 1

Problem 1-1. Many-Time Pads

Ben's system is broken. Completely. While he is not 'reusing' the pad per-se, after the 51^{st} bit, the pad is no longer random. This can be used to discern the text.

First, note the following:

- $C_x = M_x + K_x$.
- $\forall x > 50$, $K_x = K_{x \bmod 50} + \lfloor x/50 \rfloor$. That is, $K_{51} = (K_1 + 1)$, and $K_{101} = (K_1 + 2)$.
- $C_{51} - C_1 = M_5 1 - M_1 + 1$ (Etc. there are many such pairs).
- The message is probably in English, and once we see some of it, we can probably reconstruct the rest, since we believe it is book titles.
- it's possible that the last character in the message is '?', although Ben might not have bothered using it for the last book title, since it needs no seperation.

Now, although we don't know the message, or the key, we have a LOT of relationships between the characters. First off, we convert the message to numbers. We know that the fifty-first number, minus the first, minus one, yields the difference between the fifty-first message letter, and the first. We can get similar differences for all the other characters. and once we have that, we now have to resort to what we know of the English language:

- The letter 'E' is the most frequently occuring letter, and spaces are very likely to occur in sentences (or titles), also likely are 'A', 'S', and 'T'. There are books with analyses of commonality of letters in English which can be referenced.
- One very common word to look for is 'THE', especially since this is a title.

I personally reccomend the 'pick a word and look for it approach for this problem, since it can give you hints as to other lines when it works. Unsurprisingly, picking 'THE' with a space after it (not before, since it might be the beginning of a title) is a good approach, since 'THE' appears in the first column at the bottom, and gives us:

```
ON T
TION
STR
?STR
TATI
THE
```

IT's likely that this might be right, since 'TION' is a common suffix, and 'ON T' might be useful ('ON THE WATERFRONT'?). This kind of game finally yields the following titles:

- On the Origin of Species by Means of Natural Selection, or the Preservation of Favoured Races in the Struggle for Life
- A Tale of Two Cities
- The Aeneid
- Stranger in a Strange Land
- Structure and Interpretation of Computer Programs
- Sense and Sensibility
- The Lord of the Rings
- The Little Prince

and yields the key: "GOT SWEDISH OSTRICHES? THEN RIGHT ANSWER HAVE YOU."

Ben isn't going to get hired by the NSA any time soon.