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

Handout 2
September 11, 1997

Problem Set 1

This problem set is due on *Thursday, September 18, 1997* at the end of class. Late homeworks will *not* be accepted.

Mark the top of each sheet with your name, 6.857, the problem set number, and the date. Type up your solutions, and be clear. Points may be deducted if your TA has problems understanding your solution.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with. We strongly reccomend you get started on this problem set early, and work with others if possible. This may be a **DIFFICULT** problem.

Problem 1-1. Many-Time Pads

Ben Bitdiddle has been using a variation on the one-time pad described in class: Instead of

$$C_j = M_j \oplus K_j$$

he uses

$$C_j = (M_j + K_j) \bmod 30$$

Ben's system has an alphabet composed entirely of uppercase characters and a space. He then assigns a unique number to each letter or character:

$$\begin{aligned} {'space'} &= 0 \\ A &= 1 \\ B &= 2 \\ &\vdots \\ Z &= 26 \\ {'.'} &= 27 \\ {','} &= 28 \\ {'?'} &= 29 \end{aligned}$$

So if he had a key $K =$ “$ABCQ''$ and a plaintext $M =$ “$FGWX''$, the ciphertext $C =$ “$GIZK''$ would be computed thus:

$$\begin{aligned} G(7) &= A(1) + F(6) \bmod 30 \\ I(9) &= B(2) + G(7) \bmod 30 \\ Z(26) &= C(3) + W(23) \bmod 30 \\ K(11) &= Q(17) + X(24) \bmod 30 \end{aligned}$$

Dissatisfied with having to distribute new CD's all the time, Ben has developed an improvement on this system: Use the CD filled with random bits. When you run out of bits, simply add 1 to every number on the CD, and rewind to the beginning. Resume reading from the beginning of the CD. Keep doing this (the next time around, the value you use for a key will be two more than the original value on the CD).

By his computations, you should be able to use the CD 30 different times before needing a new CD. He got this after figuring out that on the 31st pass, the pad being used is the same as the pad used originally, and he knew you shouldn't re-use a pad.

Ben dropped 6.857 less than a week into class, and so never discovered that this was a bad idea. Most recently, Ben has made a list of books he likes, and encrypted them using his system.

To seperate them, Ben added a '?' character at the end of each title. Since a '?' is unlikely to occur in the middle of a title, he believes it makes for a good 'end title' character (the occurence of two of these in a row indicates that a title has ended with a question mark).

Problem: You have discovered that the CD holds 50 characters. What books does Ben like? And what are the contents of his CD? (explain what you did – especially if you want partial credit).

His encryption is:

```
V?TT.,ES.,OI?SEXIVXJVHEIHGI AN
HVI PTSGFHUZBDES .Z ,YFORXUWJJ
QFPFIX?I.,UTJFWF GSPIAFVTTXXXT
DNUWOOZF CIFLTLBNRPUPQEUD?QJIH
UUCDOGAHTABYVELF ZSVRHXHGKVBC
IGMUWJOL VTQRWWJBXLV?GCELVUBJB
,BZWYE.ZIEGKMI,HPDLEATNMHKIWSW
OSBIOLRYLYKRKLMVGCKRYA?DFB..,.
RAN,RPHIT B, EFM,MNISEJB WBQ.Q
MCYCRJANMDXRYUX,HAOV
```

note that it is available online in the course locker `/mit/6.857/psets/pset1.txt`. You should DEFINITELY get it from there to make sure you do not make any typos. Remember that spaces are characters!