Massachusetts Institute of Technology — Handout **??**
6.857: Network and Computer Security — September 17, 1998
Professor Ronald L. Rivest

Problem Set 1

This problem set is due on *Thursday, September 24, 1998* at the end of class. Late homeworks will *not* be accepted. You are to work on this problem set in groups of three to four people. (You *must* work in groups of three or four; homeworks turned in by individuals, pairs, pentuples, etc. will not be accepted. Be sure that you all understand the solutions turned in to each problem.) Mark the top of each sheet with your names, 6.857, the problem set number and question, and the date. **Type up your solutions**, and be clear. Points may be deducted if your TA has problems understanding your solution. We strongly recommend you get started on this problem set early.

Problem 1-1. Digital Postage This week, the United States Postal Service (USPS) has announced further steps to allow individuals to print postage directly onto envelopes using their home or office PC printers. Here is an earlier announcement by one of the authorized suppliers.

> After two years of developing its technology and working through the Postal Service's arduous nine-step approval process, E-Stamp said it is ready to begin beta testing the technology it created for securely delivering digital stamps - a bar code known as the Information Based Indicia, or SmartStamp - later this week in Washington, D.C. Beta trials are expected to follow in the San Francisco Bay area and Tampa, Fla.

(See `http://www.zdnet.com/intweek/daily/980401c.html`)

This would involve printing a little black, 2-dimensional "barcode" on the envelope that is going to be scanned at the postoffice. It will probably look something like this, encoding information in PDF417 format.

In a page or less, please specify the security requirements you believe necessary for this scheme. What features and protections would you desire from such a postage-stamp generating mechanism (both from the perspective of the user, and the post office)? Remember, you should focus on what security properties (policies) are desired, and not on how one would achieve those properties (mechanisms).

Problem 1-2. Break the Two-Time Pad

Can you figure out what two documents Ben has encrypted using the same one-time-pad (and what the one-time-pad is?). The following information is known:

- The encoding uses ASCII codes. With 128 possible "letters" in any position (though some are much more likely than others). For a listing of the ascii character set, you can use `man ascii` on a unix machine.
- The one-time-pad being used was pseudo-randomly generated, with values ranging from 0 to 127.
- The same pad was used to encrypt both plaintexts.
- If the plaintexts did not match in length, the shorter one was padded with spaces.
- These are both parts of relatively well known texts.

Cipher 1:

42	102	120	61	61	67	57	84	117	66	41	33	100
116	15	55	80	16	120	0	54	78	105	113	96	25
43	69	39	82	125	40	40	24	120	94	92	37	114
53	64	63	107	19	82	62	99	81	81	69	103	22
120	123	71	1	113	57	5	50	67	40	2	85	67
11	40	56	22	89	127	95	59	121	27	121	95	121
114	3	1	5	45	103	112	127	62	34	39	13	44
30	80	19	2	60	72	80	56	18	93	31	69	66
45	122	71	33	58	113	12	120	50	63	39	5	110
28	14	48	109	10	68	95	92	88	0	30	107	4
54	92	104	122	5	95	15	118	42	93	75	83	9
35	106	8	13	53	101	93	32	60	53	36	72	101
121	121	121	99	98	89	30	71	87	87	14	107	28
36	42	108	98	95	99	68	2	60				

Cipher 2:

34	40	111	117	37	64	32	88	55	74	112	117	103
121	23	54	91	5	116	84	42	79	127	35	114	80
48	67	39	71	53	62	97	12	113	48	47	34	122
57	80	63	122	77	61	93	119	68	71	83	107	87
116	115	2	19	101	112	86	127	78	109	2	89	81
17	85	5	21	94	127	84	59	109	13	42	25	116
126	7	7	18	106	118	113	62	37	63	43	102	69
73	79	14	7	105	70	17	18	25	93	56	7	27
7	84	8	117	50	123	9	44	42	50	98	76	111
6	4	48	117	7	86	88	92	75	29	16	121	65
52	80	107	50	19	8	41	46	10	84	74	95	93
57	106	27	72	125	101	73	97	56	58	51	89	101
108	125	112	99	114	72	18	9	84	30	7	107	89
34	39	103	33	86	36	3	74	104				

The two ciphertexts are available in the course locker in

```
attach 6.857
cd /mit/6.857/extra/
```

Note: It is **strongly** recommended that you do this on a computer. There is a lot of number crunching and guessing on this problem.

Problem 1-3. Snake Oil or Good Crypto?

Every once in a while, a new company is established which advertises their "perfectly secure" schemes based on the one-time pad. The latest one to have shown up is *Tristrata*. Peruse their homepage at `http://www.tristrata.com/`—and be sure to see the reference information on RKS. From the information given, can you evaluate the claims of Tristrata? If you need more information, please specify what you would like to know. (Feel free to send them email!) To the extent possible with the information available (or that you can obtain), explain why you believe the scheme to be secure, or why you believe their claims to be flawed or dubious. Would you recommend their system to a bank? To a casual user?

Limit your writeup to one page.