15-827 Security and Cryptography

Fall 2001

Homework 3 **due: Noon, October 9, 2001**

For this homework you will "crack" Manuel's PhoneOID protocol #67. Protocol 67 works as follows: H and C both know a secret, randomly chosen function $\rho : \{A, B, \ldots Z\} \to Z_{10}$, a secret, randomly chosen bijection $\pi : Z_{10} \to Z_{10}$ and a secret matrix $M \in Z_{10}^{3\times 3}$. To authenticate H, C randomly picks a challenge vector $c \leftarrow \{A, \ldots, Z\}^3$ and sends it to H. H then computes the column vector d given by $d_i = \rho(c_i)$; the vector $e = Md$, and the vector r defined by $r_i = \pi(e_i)$. H responds to C with the vector r, and C accepts if the value is correct. Below are some values of c and r for Manuel's secrets:

```
the red fox bit nst dog who ate his ear off bnl sol qmn bnx usd ubh xyp cjk vzp
423 312 354 057 902 395 215 507 501 570 434 253 914 152 330 791 535 190 797 653
```

Your job is to produce a program which can respond to a challenge with Manuel's response, with probability $\frac{1}{100}$ or better. Your program will take a three-lowercase-letter challenge as a command-line argument and produce a list of at most 100 possible responses. To assess your program, it will be evaluated at 100 random challenges. Let C be the number of times your program lists the correct response in its output. Let T be the total number of responses output by your program. Then your grade will be determined by the ratio $r = C/T$ according to the following chart:

$0 \leq r < 1/200$	0
$1/200 \leq r < 1/100$	15
$1/100 \leq r < 1/50$	$25 - \frac{1}{20r}$
$1/50 \leq r < 1/10$	$25.5 - \frac{1}{16r}$
$1/10 \leq r \leq 1$	$30 - \frac{1}{2r}$

The programming portion of the assignment will be graded out of 25 points.

There is also a written portion to this assignment. In this portion you will describe in detail how your program works and whatever precomputations were necessary to prepare your program. You may also describe any computations you were unable to perform but which would allow you to produce a better program with less work than 10^{15} - about a day's worth of supercomputer time - and fewer than 50 challenge-response pairs. The written portion will be graded out of 25 points, with points awarded for clarity, correctness, and the success probability for the best attack you can describe.

To turn in your assignment, please send (via email) a tarred and compressed file named `<username>.tar.gz` to `hopper@cs.cmu.edu` by noon EDT on Tuesday 9 October 2001. This tarball should untar to a directory named `<username>` which contains a file `runme` which will execute on an i386 linux machine, and takes a single, three-letter challenge on the command line. The directory should also contain a postscript or pdf file named `writeup.ps` (resp, `.pdf`) which has the written portion of your assignment.