MATH 295A/395A: CRYPTOGRAPHY
HOMEWORK #5

Problems for all

Problem 1. Let

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 10 \end{pmatrix}.$$

(a) For which n is the matrix A invertible over $\mathbb{Z}/n\mathbb{Z}$?

(b) Find its inverse if $n = 100$. How many operations in $\mathbb{Z}/n\mathbb{Z}$ (i.e., $+$, $-$, $*$, $^{-1}$) does it take to compute this inverse?

Problem 2. Suppose the matrix $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ is mistakenly used for an encryption matrix in a Hill cipher (with $n = 26$). Find two plaintexts that encrypt to the same ciphertext.

Problem 3. The plaintext message

Consistency is the last refuge of the unimaginative

is encrypted using a Hill cipher with with $k = 3$ (and $n = 26$) to get the ciphertext

`voqimugocogmttfkxvlvdynhawugtfrsksoizgaanlygk`

Determine the key $A \in M_3(\mathbb{Z}/26\mathbb{Z})$. The matrix key spells out a keyword: what is it?

Problem 4. The Hill cipher succumbs to a known plaintext attack if sufficient plaintext-ciphertext pairs are provided. It is even easier to break the Hill cipher if Eve can trick Alice into encrypting a chosen plaintext: this is known as a *chosen plaintext attack*. Describe such an attack.

Problem 5. Convert the top secret password

a6@1!*Hj

into a string of ASCII bytes, then write this string as an element of $(\mathbb{Z}/65537\mathbb{Z})^4$.

Additional problems for 395A

Problem 6. What is the probability that a randomly chosen matrix $A \in M_2(\mathbb{Z}/p\mathbb{Z})$ is invertible, where p is prime?

Problem 7. Let F be a field and $k \in \mathbb{Z}_{>0}$. Find an explicit polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 in such that no more than $f(k)$ operations in F are required by the row-reduction algorithm for computing the determinant of a matrix in $M_k(F)$. How many of these operations are inversions?

Date: Due Wednesday, 8 October 2008.