

**MATH 75: MATHEMATICAL CRYPTOGRAPHY  
HOMEWORK #4**

PROBLEMS

**Problem 1.** Let

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

For which  $n$  is the matrix  $A$  invertible over  $\mathbb{Z}/n\mathbb{Z}$ ? Find its inverse if  $n = 100$ .

**Problem 2.** Alice uses the Hill cipher, encrypting the plaintext

Consistency is the last refuge of the unimaginative

to get the ciphertext

voqimugocogmttfkxvldynhawugtfrsksoizgaanlygk

to send to Bob using blocks of size  $m = 3$  (and  $n = 26$ ). Playing the role of Eve, hack Alice's encryption key  $A \in M_3(\mathbb{Z}/26\mathbb{Z})$ . The matrix key spells out a keyword: what is it?

After you find the key, notice that Alice has not followed the protocol correctly. Find two plaintexts that encrypt to the same ciphertext.

**Problem 3.** The Hill cipher succumbs to a known plaintext attack if sufficiently many plaintext-ciphertext pairs are known. It is even easier to break the cipher if Eve can trick Alice into encrypting a chosen plaintext, a *chosen plaintext attack*. Describe such an attack.

**Problem 4.** Let  $n \in \mathbb{Z}_{>0}$ . We consider the row-reduction algorithm over  $\mathbb{Z}/p\mathbb{Z}$  where  $p$  is prime. Show that every nonzero element in  $\mathbb{Z}/p\mathbb{Z}$  has an inverse, so that  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  is a *field* and the methods of linear algebra apply.

Find an explicit polynomial  $f(x) \in \mathbb{Q}[x]$  of degree 3 such that no more than  $f(n)$  operations in  $\mathbb{F}_p$  are required by the row-reduction algorithm for computing the determinant of a matrix in  $M_n(\mathbb{F}_p)$ . How many of these operations are inversions?

**Problem 5.** Decrypt the message

CLV SSH = MMBVC RDMVE PFZII EAVYS XFTHS FNMOB RRPDH VBSQH

with the following Enigma settings:

Walzenlage (Rotors): I V III

Ringstellung (Ring setting): 13 06 24

Steckerverbindungen (Plug connections): AU PB EF IQ RH ZL DT MS CG KN

Kennggruppen: KIJ TFR BVC ZAE

[Hint: The message is in German!]

**Problem 6.** Read Section 15.1 (pages 368–376) of *The Pleasures of Counting* by Koerner (<http://www.math.dartmouth.edu/~m75s16/koerner.pdf>) and do Exercises 15.1.1–15.1.3.