MATH 295B/395A: CRYPTOGRAPHY
HOMEWORK #4

Problem 1. Consider the affine cipher with $\mathcal{P} = \mathcal{C} = \mathbb{Z}/n\mathbb{Z}$.

(a) Suppose $n = 541$ and we take the key $(a, b) = (34, 71)$. Encrypt the plaintext $m = 204$, and decrypt the ciphertext $c = 431$.

(b) Eve intercepts a ciphertext from Alice and through espionage she learns that the letter $x \in \mathcal{P}$ is encrypted as $y \in \mathcal{C}$ in this message. Show that Eve can decrypt the message using $O(n)$ trials.

(c) Now suppose that (contrary to Kirchoff's principle) the integer n is not public knowledge. Is the affine cipher still vulnerable if Eve manages to steal a plaintext/ciphertext pair? How might Eve break the system?

Problem 2. Encrypt the message

Why is a raven like a writing desk

using the Vignère cipher with keyword `rabbithole`. [*Hint: Use a Vigenère tableau!*]

Problem 3. [Sage] Decrypt the following message, which was encrypted using a Vignère cipher.

```
mgodt beida psgls akowu hxukc iawlr csoyh prtrt udrqh cengx
uuqtu habxw dgkie ktsnp sekld zlvnh wefss glzrn peaoy lbyig
uaafv eqgjo ewabz saawl rzjpv feyky gylwu btlyd kroec bpfvt
psgki puxfb uxfuq cvymy okagl sactt uwlrx psgiy ytpsf rjfuw
igxhr oyazd rakce dxeyr pdobr buehr uwcue ekfic zehrq ijezr
xsyor tcylf egcy
```

(a) Use the method of displacement coincidences to guess the key length.

(b) Use the Kasiski test of matching trigrams to give more evidence for your guess for the key length.

(c) Use frequency analysis with the guessed key length to decrypt the message.

Computational problem

Problem 4. Write a computer program that takes as input positive integers r, a and produces as output the r-adic expansion of a.

Date: Due Friday, 24 September 2010.

Problem 5. Consider the quadratic map

$$\begin{aligned} E : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ x &\mapsto x^2 + ax + b \end{aligned}$$

with $a, b \in \mathbb{Z}/n\mathbb{Z}$. Show that if $n \neq 2$, then E is *never* an encryption function. What can you say about other maps $x \mapsto f(x)$ where $f(x) \in \mathbb{Z}[x]$?

Problem 6. Let $D_n = \{x \in \mathbb{R}^n : \sum_{i=1}^n x_i^2 = 1\}$. Let $x \in D_n$. Consider the map

$$\begin{aligned} D_n &\to \mathbb{R} \\ y &\mapsto x \cdot y = \sum_{i=1}^n x_i y_i. \end{aligned}$$

Show that this function achieves a unique maximum at $x = y$. [*Hint: If this is super hard, just do the case* $n = 2$.]