PMAT 4282 – Cryptography Assignment #3
Winter 2009

Instructions

- Answer each question completely; justify your answers.
- This assignment is due at: 3:00 pm on Thursday 05 February 2009.

1. For each integer $x \in \mathbb{Z}_{26}$ such that $\mathrm{GCD}(x, 26) = 1$, calculate x^{-1} modulo 26.

2. Suppose that M is a square matrix over $\mathbb{Z}_n$.
   Prove that if M^{-1} exists then $\mathrm{GCD}(\det(M), n) = 1$.

3. Consider the plaintext "*surely she sells sea shells by the sea shore*".

   (a) Determine the index of coincidence of the plaintext.

   (b) Encrypt the plaintext using the Vigenère cipher, with "*RUSTY*" as the keyword, and determine the index of coincidence of the corresponding ciphertext.

   (c) Encrypt the plaintext using the Hill cipher, with $\begin{bmatrix} 1 & 17 & 4 \\ 0 & 19 & 7 \\ 19 & 0 & 10 \end{bmatrix}$ as the key, and determine the index of coincidence of the corresponding ciphertext.

4. Suppose you intercept the following ciphertext:

   BLPZQFSNEQLOOCMXHCVVNNKTGMDFCKIWLNRBXH

   You know the ciphertext was generated via the Hill cipher but you do not know the key. However, you have been able to ascertain that the corresponding plaintext is likely to be:

   january twenty-sixth. ten am. no enemy activity.

   Determine the key that is being used, assuming that the key is a 2 by 2 matrix.

5. The Hill cipher requires that the key matrix be invertible, modulo 26. Find three distinct matrices, K_1, K_2, and K_3, such that $xK_1 = xK_2 = xK_3$ for the plaintext string $x =$ "*th*". Which of your matrices is invertible?

Definition: A *field* $(\mathcal{F}, +, \cdot)$ consists of a set $\mathcal{F}$ along with two binary operations, $+$ and $\cdot$, such that:

- $\mathcal{F}$ is closed under both $+$ and $\cdot$
- $+$ and $\cdot$ are both commutative (i.e., $a + b = b + a$ and $a \cdot b = b \cdot a$)
- $+$ and $\cdot$ are both associative (i.e., $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$)
- $\cdot$ distributes over $+$ (i.e., $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$)
- there exists an element $1 \in \mathcal{F}$ such that $a \cdot 1 = a$ for all $a \in \mathcal{F}$
- there exists an element $0 \in \mathcal{F}$ such that $a + 0 = a$ for all $a \in \mathcal{F}$
- for each $a \in \mathcal{F}$ there exists an element $(-a) \in \mathcal{F}$ such that $a + (-a) = 0$
- for each $a \in \mathcal{F}$ such that $a \neq 0$, there exists an element $a^{-1} \in \mathcal{F}$ such that $a \cdot a^{-1} = 1$

Note that when there is no confusion concerning $+$ and $\cdot$, we often refer to the field as $\mathcal{F}$ rather than $(\mathcal{F}, +, \cdot)$.

(over)

6. Determine whether each of the following is a field. Justify your answers.

   (a) $\mathbb{Z}$, using standard arithmetic

   (b) $\mathbb{Q}$, using standard arithmetic

   (c) $\mathbb{Z}_{26}$, using modular arithmetic (modulo 26)

   (d) $\mathbb{Z}_p$, where p is prime, using modular arithmetic (modulo p)

   (e) $\{0\}$, using standard arithmetic

Fact: A matrix M over a field $\mathcal{F}$ is invertible if and only if the rows of M are linearly independent.

7. How many 2×2 matrices are there that are invertible over $\mathbb{Z}_{26}$?
   (i.e., how large is the keyspace for the Hill cipher when $m = 2$)?

8. Exercise 1.12 of Stinson: Let p be a prime. Show that the number of 2×2 matrices that are invertible over $\mathbb{Z}_p$ is $(p^2 - 1)(p^2 - p)$.

9. Exercise 1.14 of Stinson: A matrix M is called involutory if $M = M^{-1}$. Regarding the Hill cipher, if Alice and Bob selected the key matrix k to be involutory, it would save them from also having to determine the inverse of k.

   (a) Suppose that M is an involutory matrix over $\mathbb{Z}_{26}$.
   Prove that either $\det(M) \equiv 1 \pmod{26}$ or $\det(M) \equiv -1 \pmod{26}$.

   (b) Determine the number of 2×2 involutory matrices over $\mathbb{Z}_{26}$.