Workshop 1: Ciphers

3CC: Codes and Ciphers (530.334)

28th July, 2005

1. Let $a, b \in \mathbb{Z}_n$ and define a function $e : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $e(x) = ax + b$.

(a) Show that if $\gcd(a, n) \neq 1$ then $e$ is not one-to-one.

(b) Show that if $\gcd(a, n) = 1$ then $e$ is one-to-one.

This shows that an affine cipher (with $n = 26$) is one-to-one if and only if $\gcd(a, 26) = 1$ (which is true if and only if $a$ is odd and not 13).

2. Encrypt ‘So you thought you had seen the back of permutations forever after 3P5 did you?’ using a permutation cipher with key

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

What is the decryption key?

3. A Hill cipher has key an $n \times n$ matrix $M$ with entries in $\mathbb{Z}_{26}$. Encryption is done by converting the message string to integers in $\mathbb{Z}_{26}$ in the usual way, and then breaking the message into strings of length $n$. For each string $\mathbf{x} = (x_1, \ldots, x_n)$ we then find the product $\mathbf{x}M$, and convert the result back into letters.

(a) Use

$$
M = \begin{pmatrix} 0 & 3 & 0 \\
0 & 0 & 21 \\
15 & 0 & 0 \end{pmatrix}
$$

to encrypt ‘artichoke’.

(b) Prove that

$$
\begin{pmatrix} 0 & 0 & 7 \\
9 & 0 & 0 \\
0 & 5 & 0 \end{pmatrix}
$$

is the decryption key.

(c) Is

$$
\begin{pmatrix} 3 & 0 & 1 \\
9 & 5 & 7 \\
17 & 1 & 3 \end{pmatrix}
$$

a valid key for a Hill cipher? (why or why not?)