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.

Assume that \( \gcd(a, n) = d > 1 \). We want to show that there exist two different elements of \( \mathbb{Z}_n \) which are mapped by \( e \) to the same element. As an educated guess, choose \( x_1 = 0 \) and \( x_2 = n/d \). Since \( 0 < n/d < n \), \( x_2 \) is not congruent to \( 0 \) \((\text{mod} \ n)\), and so \( x_1 \neq x_2 \). Now \( ax_1 + b \equiv b \) \((\text{mod} \ n)\) and \( ax_2 + b \equiv a \frac{n}{d} + b \equiv \frac{a}{d}n + b \equiv b \) \((\text{mod} \ n)\). So \( e(x_1) = e(x_2) \), and hence \( e \) is not one-to-one.

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

Assume that \( \gcd(a, n) = 1 \) and that \( e(x_1) = e(x_2) \) for some \( x_1, x_2 \in \mathbb{Z}_n \). Then \( ax_1 + b \equiv ax_2 + b \) \((\text{mod} \ n)\) which implies that \( a(x_1 - x_2) \equiv 0 \) \((\text{mod} \ n)\). Since \( \gcd(a, n) = 1 \) we can divide both sides of the congruence by \( a \), giving \( (x_1 - x_2) \equiv 0 \) \((\text{mod} \ n)\). Hence \( x_1 = x_2 \) and \( e \) 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

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

Write out the first block of 8 letter with the permutation underneath, and move the \( i^{th} \) letter to the \( \pi(i)^{th} \) position, (ie move the 1st letter to the 4th position, the 2nd to the 6th and so on) as follows:
Then do the same for the remaining blocks of 8 letters, and join together to get the ciphertext.

What is the decryption key?

The inverse permutation $\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 4 & 1 & 3 & 2 & 7 & 6 \end{pmatrix}$.

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 $x = (x_1, \ldots, x_n)$ we then find the product $xM$, 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’.

(Note that all multiplication is done mod 26.) The message ‘artichoke’ as integers in $\mathbb{Z}_{26}$ is $0 \ 17 \ 19 \ 8 \ 2 \ 7 \ 14 \ 10 \ 4$. Multiplying the first string of length 3 by $M$ gives

$$(0,17,19).M = (285,0,359) \equiv (25,0,19) \pmod{26}.$$

Continuing in the way we obtain the string $25 \ 0 \ 19 \ 1 \ 24 \ 16 \ 8 \ 16 \ 2$ which yields the ciphertext ZATBYQIQC.

(b) Prove that $\begin{pmatrix} 0 & 0 & 7 \\ 9 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$ is the decryption key.

To decrypt after encrypting with $M$, we multiply by $M^{-1}$; ie we use the fact that $xMM^{-1} = x$. So we show that $\begin{pmatrix} 0 & 0 & 7 \\ 9 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix} = M^{-1}$.

$$\begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 21 \\ 15 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 7 \\ 9 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix} = \begin{pmatrix} 105 & 0 & 0 \\ 0 & 27 & 0 \\ 0 & 0 & 105 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \pmod{26}.$$
(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?)

No it isn’t, because the determinant is 0 and hence there is no decryption key. (Note that having non-zero determinant is necessary but not sufficient for a matrix $A$ over $\mathbb{Z}_{26}$ to be a valid key for a Hill cipher. A necessary and sufficient condition is that $\gcd(26, \det(A)) = 1$.)