1. Given sets $S$ and $T$, let $\text{Hom}(S,T)$ denote the set of all functions $f : S \rightarrow T$. Prove that the map
\[ R : \text{Hom}(X \times Y, Z) \longrightarrow \text{Hom}(X, \text{Hom}(Y, Z)), \]
is a bijection, where $R(f)(x)$ is defined to be the map $y \mapsto f(x,y)$.

**Hint:** Write down the inverse map $L$ to $R$, and show that each of $L \circ R$ and $R \circ L$ are identity maps. In particular, for any $f$ in the domain observe that $R(f)(x)(y) = f(x,y)$ for all $x \in X$ and $y \in Y$, and similarly for any $g$ in the codomain, let $L(g)$ be the function such that $L(g)(x,y) = g(x)(y)$. To show that two functions in the domain are equal, it suffices to show that they agree at all $(x, y) \in X \times Y$.

**Remark:** Using this “natural” bijection, we identify the function $E$ of a cryptosystem either with a function $K \times M \rightarrow C$ or with a function $K \rightarrow \text{Hom}(M, C)$. Under the latter identification, recall that we call the maps $E(K)$ the set of ciphers of the cryptosystem.

**Solution** We set $L(g)(x, y) = g(x)(y)$, and show that $L(R(f)) = f$ and $R(L(g)) = g$ for all $f$ in the domain of $R$ and $g$ in the codomain. To show that two functions are equal it suffices to show that they agree on all elements of the (common) domain.

Given $f : X \times Y \rightarrow Z$, we check that
\[ L(R(f))(x, y) = R(f)(x)(y) = f(x,y), \]
for all $(x, y)$ in $X \times Y$. Thus $L(R(f)) = f$. This proves that $R$ is injective. Similarly, given $g : X \rightarrow \text{Hom}(Y, Z)$, we want to determine if the equality
\[ R(L(g))(x) = g(x) \]
holds for all $x$ in $X$. In both cases this is a function $Y \rightarrow Z$, so we just need to check that the evaluation of both sides is equal at all $y$ in $Y$. But this holds by definition of $L$:
\[ R(L(g))(x)(y) = L(g)(x, y) = g(x)(y) \]
so $R(L(g)) = g$. This proves that $R$ is surjective, hence a bijection.

2. A subset $S$ of a monoid $\mathcal{M}$ is itself a monoid if $S$ contains the identity element $e$ and is closed under the monoid operation – i.e. for every $x$ and $y$ in $S$, the product $xy$ is contained in $S$. Such a subset is called a submonoid.

**a.** Let $\mathcal{A}$ be a finite alphabet, and $\mathcal{A}^*$ the string monoid on $\mathcal{A}$. Show that the subset $\mathcal{A}^n$ of strings of length $kn$ for integers $k \geq 0$ forms a submonoid.

**b.** Show that the obvious map from $\phi : (\mathcal{A}^n)^* \rightarrow \mathcal{A}^*$ mapping onto $\mathcal{A}^n$ is a monoid homomorphism (i.e. takes the identity element to the identity element and preserves products).

**c.** Define an injective map $\psi : \mathcal{A}^* \rightarrow \mathcal{A}^n$ — such a map is often called a padding. Is your map a monoid homomorphism? Can there exist a padding which is both a homomorphism, and restricts to the identity map on the submonoid $\mathcal{A}^n$?
Solution

a. The subset $\mathcal{A}_n$ equals
\[
\bigcup_{k \geq 0} \mathcal{A}^{kn},
\]
which contains the empty string (the identity element) and is closed under multiplication (the concatenation of a string of length $kn$ and length $mn$ has length $(k+m)n$, which is again in $\mathcal{A}_n$. Thus it forms a submonoid.

b. The “obvious” map takes a string in $\mathcal{A}_n$ consisting of $k$ elements from $\mathcal{A}_n$, each of length $n$, to the concatenated string of length $kn$. We can think of this map as dropping the parenthesis around blocks of length $n$ (each in $\mathcal{A}_n$). If one concatenates two strings in $\mathcal{A}_n$ and drops parentheses, this gives the same as dropping the parentheses and concatenating the strings. Thus the inclusion preserves multiplication. Similarly, the identity elements in each case is the empty string (i.e. the string of length zero). The empty string in $\mathcal{A}_n^*$ clearly maps to the empty string in $\mathcal{A}_n^*$ under this map. It follows that this “obvious” inclusion is a homomorphism.

c. One injective map $\psi : \mathcal{A}_n^* \to \mathcal{A}_n$ is that which appends one $\mathcal{A}$ and from $0$ to $n-1$ characters $Z$ to a string. The inverse map $\pi : \mathcal{A}_n \to \mathcal{A}_n^*$ truncates all trailing $Z$s and then removes the final $\mathcal{A}$. Checking that $\pi \psi$ is the identity on $\mathcal{A}_n^*$, we conclude that $\psi$ is injective.

3. Let $\mathcal{A}$ be the alphabet of symbols $\{A, B, \ldots, Z\}$, identified with the set $\mathbb{Z}/26\mathbb{Z}$.

a. Define a map $\mathcal{A}^2 \to \mathcal{A}^2$ by $x_1x_2 \mapsto y_1y_2$, where
\[
\begin{align*}
  y_1 &= 3x_1 + x_2 + 1 \\
  y_2 &= x_1 + 2x_2 + 3
\end{align*}
\]
Find an inverse to this map (with similar expression). What are the images of $\mathcal{A}^N$, $\mathcal{I}T$, and $\mathcal{A}T$ under this map?

b. Note that this map can be defined by $(x_1, x_2) \mapsto (y_1, y_2) = (x_1, x_2)A + (1, 3)$, where $A$ is the matrix
\[
\begin{pmatrix}
  3 & 1 \\
  1 & 2
\end{pmatrix}.
\]
A map $(x_1, x_2) \mapsto (x_1, x_2)A$ is called a matrix transformation and a map of the form $(z_1, z_2) \mapsto (z_1, z_2) + (w_1, w_2)$ is called a translation. What substitution ciphers be expressed in this way (as a matrix transformation and by a translation)?

c. Find an expression for the transposition cipher with key $\sigma = (1, 3, 2, 4)$, written in cycle notation, as a matrix transformation $\mathcal{A}^4 \to \mathcal{A}^4$.

Solution The inverse to $(x_1, x_2) \mapsto (x_1, x_2)A + (1, 3)$ is the map
\[
(y_1, y_2) \mapsto ((y_1, y_2) - (1, 3))A^{-1},
\]
where $A^{-1}$ is inverse matrix to $A$, which takes the form
\[
A^{-1} = \frac{1}{5} \begin{pmatrix}
  2 & -1 \\
  -1 & 3
\end{pmatrix}.
\]
Noting that “1/5” is the element such that $1/5 \cdot 5 = 1$ in $\mathbb{Z}/26\mathbb{Z}$, and that $5 \cdot 5 = 25 = -1$, it follows that $1/5 = -5$ in $\mathbb{Z}/26\mathbb{Z}$, and

$$A^{-1} = \begin{pmatrix} 16 & 5 \\ 5 & 11 \end{pmatrix}.$$  

If we then expand the inverse map, we get

$$(y_1, y_2) \mapsto (y_1, y_2) \begin{pmatrix} 16 & 5 \\ 5 & 11 \end{pmatrix} - (5, 12) = (16y_1 + 5y_2 + 21, 5y_1 + 11y_2 + 14)$$

The pairs AN, IT, and AT correspond to vectors $(x_1, x_2) = (0, 13), (8, 19), (0, 19)$, which map to $(y_1, y_2) = (14, 3) = \text{OD}, (18, 23) = \text{SX},$ and $(20, 15) = \text{UP}$. (Or, setting $(y_1, y_2) = (0, 13), (1, 19),$ and $(0, 19)$, the inverse map takes AN, IT, and AT to $(8, 1) = \text{IB}, (10, 3) = \text{KD},$ and $(12, 15) = \text{MP}$).

Note that this is not a substitution cipher, since the image of the first (or second) character depends on the second (or first, respectively). Moreover the same permutation map must be applied to $x_1$ and $x_2$ to yield $y_1$ and $y_2$, respectively, in other words:

$$(x_1, x_2) \mapsto (x_1, x_2) \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + (b, b) = (ax_1 + b, ax_2 + b).$$

These are precisely the affine substitution ciphers. There are many more substitutions (permutations of $\{A, \ldots, Z\}$) than just the affine substitutions. However, the affine substitution ciphers generalise as above to linear (or affine) substitutions in any number of characters, which provides a “mixing” of the plaintext characters.

4. Find the element $x$ of $\mathbb{Z}/35\mathbb{Z}$ which corresponds to $y = (2, 3)$ under the Chinese remainder theorem map:

$$\pi : \mathbb{Z}/35\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$  

For $e = 5$, determine $x^e$ and $y^e$ and show that $\pi(x^e) = y^e$, and find $d$ such that $y^{ed} = y$ (and hence $x^{ed} = x$).

Solution The element $x = 17$ maps to $y = (2, 3)$ by noting that $17 \mod 5 = 2$ and $17 \mod 7 = 3$. Using the relation

$$3 \cdot 5 + (-2) \cdot 7 = 1,$$

the element $x$ is given by

$$x = 2 + (3 - 2) \cdot (3 \cdot 5) = 3 + (2 - 3) \cdot (-2 \cdot 7) = 17 \mod 35.$$  

One calculates $x^e = 17^5 \mod 35 = 12$, while

$$y^e = (2^5 \mod 5, 3^5 \mod 7) = (2, 5).$$

Finally we note that $d = 5$ is the smallest positive integer solving the two equations $ed \mod (5 - 1) = 1$ and $ed \mod (7 - 1) = 1$ (for $e = 5$), hence $x^{ed} = x$ and $y^{ed} = y$. 