1 Cryptography: An Overview

1.4 The Hill Cipher

Problem 1. *Complete the following:*

(a) Use a 26-character Hill cipher to encode the message `FOUR` *using the key matrix* $K = \begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}$.

(b) Let $\alpha_1\alpha_2\alpha_3\alpha_4$ *represent your answer from part (a). Now encode the message* $\alpha_1\alpha_2\alpha_3\alpha_4$ *using the same key matrix that you used in part (a).*

(c) There should be something surprising about your answer in part (b). Is that simply a coincidence? Explain.

Let's start with part (a). To encode the message `FOUR` using the provided Hill cipher, we'll rewrite the phrase into two-letter vectors according to $A \mapsto 0, B \mapsto 1, \ldots,$ and so on:

$$\texttt{FO} \mapsto \begin{pmatrix} 5 \\ 14 \end{pmatrix} = \mathbf{x_1}, \quad \texttt{UR} \mapsto \begin{pmatrix} 20 \\ 17 \end{pmatrix} = \mathbf{x_2}.$$

We'll then multiply each as $K\mathbf{x_1}, K\mathbf{x_2}$ and reduce to their representatives modulo 26:

$$K\mathbf{x_1} = \begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 5 \\ 14 \end{pmatrix} = \begin{pmatrix} 125 \\ 24 \end{pmatrix} \equiv \begin{pmatrix} 21 \\ 24 \end{pmatrix} = \mathbf{y_1},$$

$$K\mathbf{x_2} = \begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 20 \\ 17 \end{pmatrix} = \begin{pmatrix} 500 \\ 57 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 5 \end{pmatrix} = \mathbf{y_2}.$$

Finally, we can map these vectors back to their corresponding digrams, completing the encryption:

$$\mathbf{y_1} = \begin{pmatrix} 21 \\ 24 \end{pmatrix} \mapsto \texttt{VY}, \quad \mathbf{y_2} = \begin{pmatrix} 6 \\ 5 \end{pmatrix} \mapsto \texttt{GF}.$$

Thus our encrypted message is `VYGF`.

For part (b), we'll perform the same process as above:

$$K\mathbf{y_1} = \begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 21 \\ 24 \end{pmatrix} = \begin{pmatrix} 525 \\ 66 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 14 \end{pmatrix} = \mathbf{z_1},$$

$$K\mathbf{y_2} = \begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 150 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 17 \end{pmatrix} = \mathbf{z_2}.$$

$$\mathbf{y_1} = \begin{pmatrix} 5 \\ 14 \end{pmatrix} \mapsto \texttt{FO}, \quad \mathbf{y_2} = \begin{pmatrix} 20 \\ 17 \end{pmatrix} \mapsto \texttt{UR}.$$

As a result, we get the original plaintext `FOUR`. Looking to part (c), we can see that the linear transformation, K, is it's own inverse modulo 26:

$$\begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 25 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 625 & 0 \\ 52 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{26}$$

which confirms that KK will result in the original vector modulo 26.

Problem 2. *Alice and Bob agree that they will use a Hill Cipher to send messages to each other. They decide to use* $K = \begin{pmatrix} 2 & 1 \\ 3 & 6 \end{pmatrix}$ *for the key matrix. Bob receives the ciphertext* `SMKH` *from Alice. What is the plaintext?*

To find the plaintext, we simply need to calculate K^{-1} and apply it to the digram's corresponding vector:

$$K^{-1} = \frac{1}{2(6) - 1(3)} \begin{pmatrix} 6 & -1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 2/3 & -1/9 \\ -1/3 & 2/9 \end{pmatrix}$$

Using the mapping `SM` $\mapsto \begin{pmatrix} 18 \\ 12 \end{pmatrix}$ and `KH` $\mapsto \begin{pmatrix} 10 \\ 7 \end{pmatrix}$

1.5 Attacks on the Hill Cipher

Problem 1. *You discover*[1] *that the key matrix for a certain Hill cipher is* $K = \begin{pmatrix} 8 & 1 \\ 1 & 2 \end{pmatrix}$. *You have intercepted the ciphertext* `BYIC`. *What is the plaintext?*

Answer here...

Problem 2. *You have intercepted the message*

`WGTK`

and know it has ben encrypted using a Hill cipher. You also happen to know that `CD` *is encrypted as* `RR` *and* `JK` *is encrypted as* `OV`. *What is the plaintext?*

Answer here...

1.6 Feistel Ciphers and DES

Problem 1. *Consider the fifth S-box used in DES. Think of it as a function from* $\mathbb{Z}_2^6$ *to* $\mathbb{Z}_2^4$. *Show that this function is not linear.*

Answer here...

[1] How convenient!