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 $A \mapsto 0, B \mapsto 1, \dots,$ 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. Knowing that the determinant is $2(6) - 1(3) = 9$:

$$K^{-1} = 9^{-1} \begin{pmatrix} 6 & -1 \\ -3 & 2 \end{pmatrix} \equiv 3 \begin{pmatrix} 6 & 25 \\ 23 & 2 \end{pmatrix} \equiv \begin{pmatrix} 18 & 23 \\ 17 & 6 \end{pmatrix} \pmod{26}$$

Using the mapping `SM` $\mapsto \begin{pmatrix} 18 \\ 12 \end{pmatrix} = \mathbf{y_1}$ and `KH` $\mapsto \begin{pmatrix} 10 \\ 7 \end{pmatrix} = \mathbf{y_2}$ we'll calculate $K^{-1}\mathbf{y_1}$ and $K^{-1}\mathbf{y_2}$:

$$K^{-1}\mathbf{y_1} = \begin{pmatrix} 18 & 23 \\ 17 & 6 \end{pmatrix} \begin{pmatrix} 18 \\ 12 \end{pmatrix} = \begin{pmatrix} 600 \\ 378 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \mathbf{x_1},$$

$$K^{-1}\mathbf{y_2} = \begin{pmatrix} 18 & 23 \\ 17 & 6 \end{pmatrix} \begin{pmatrix} 10 \\ 7 \end{pmatrix} = \begin{pmatrix} 341 \\ 212 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \mathbf{x_2}.$$

Mapping these vectors back to their digrams, we get the plaintext `CODE`.

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?*

We can use the same procedure from problem 2 of section 1.4 to crack the code. Knowing that $det(K) = 15$, we can determine that

$$K^{-1} = 15^{-1} \begin{pmatrix} 2 & -1 \\ -1 & 8 \end{pmatrix} = 7 \begin{pmatrix} 2 & 25 \\ 25 & 8 \end{pmatrix} \equiv \begin{pmatrix} 14 & 19 \\ 19 & 4 \end{pmatrix} \pmod{26}$$

Using the mapping `BY` $\mapsto \begin{pmatrix} 1 \\ 24 \end{pmatrix} = \mathbf{y_1}$ and `IC` $\mapsto \begin{pmatrix} 8 \\ 2 \end{pmatrix} = \mathbf{y_2}$ we'll calculate $K^{-1}\mathbf{y_1}$ and $K^{-1}\mathbf{y_2}$:

$$K^{-1}\mathbf{y_1} = \begin{pmatrix} 14 & 19 \\ 19 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 24 \end{pmatrix} = \begin{pmatrix} 470 \\ 115 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 11 \end{pmatrix} = \mathbf{x_1},$$

$$K^{-1}\mathbf{y_2} = \begin{pmatrix} 14 & 19 \\ 19 & 4 \end{pmatrix} \begin{pmatrix} 8 \\ 2 \end{pmatrix} = \begin{pmatrix} 150 \\ 160 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 4 \end{pmatrix} = \mathbf{x_2}.$$

Mapping these vectors back to their digrams, we get the plaintext `CLUE`.

[1] How convenient!

Problem 2. *You have intercepted the message*

$$\texttt{WGTK}$$

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?*

Let's first map these digrams to vectors in $\mathbb{R}^2$ and combine them into a matrix:

$$\texttt{CD},\texttt{JK} \mapsto \begin{pmatrix} 2 & 9 \\ 3 & 10 \end{pmatrix}; \quad \texttt{RR},\texttt{OV} \mapsto \begin{pmatrix} 17 & 14 \\ 17 & 21 \end{pmatrix}.$$

We know that the first matrix is linearly-mapped to the second via a Hill cipher's key matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 9 \\ 3 & 10 \end{pmatrix} = \begin{pmatrix} 17 & 14 \\ 17 & 21 \end{pmatrix}.$$

Next, let's calculate the inverse of the plaintext matrix:

$$\begin{pmatrix} 2 & 9 \\ 3 & 10 \end{pmatrix}^{-1} = (-7)^{-1}\begin{pmatrix} 10 & -9 \\ -3 & 2 \end{pmatrix} \equiv 19\begin{pmatrix} 10 & 17 \\ 23 & 2 \end{pmatrix} = \begin{pmatrix} 110 & 187 \\ 253 & 22 \end{pmatrix} \equiv \begin{pmatrix} 6 & 5 \\ 19 & 22 \end{pmatrix} \pmod{26}.$$

We can then multiply both sides from the right by the inverse of the plaintext matrix:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 2 & 9 \\ 3 & 10 \end{pmatrix}\begin{pmatrix} 6 & 5 \\ 19 & 22 \end{pmatrix} &= \begin{pmatrix} 17 & 14 \\ 17 & 21 \end{pmatrix}\begin{pmatrix} 6 & 5 \\ 19 & 22 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= \begin{pmatrix} 17 & 14 \\ 17 & 21 \end{pmatrix}\begin{pmatrix} 6 & 5 \\ 19 & 22 \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 368 & 393 \\ 501 & 547 \end{pmatrix} \\ &\equiv \begin{pmatrix} 4 & 3 \\ 7 & 1 \end{pmatrix} \pmod{26}. \end{aligned}$$

This resulting matrix $\begin{pmatrix} 4 & 3 \\ 7 & 1 \end{pmatrix}$ is the Hill cipher key. To finally decrypt, we must first invert this key, noting the determinant is $-17 \equiv 9 \pmod{26}$:

$$K^{-1} = \begin{pmatrix} 4 & 3 \\ 7 & 1 \end{pmatrix}^{-1} = 9^{-1}\begin{pmatrix} 1 & -3 \\ -7 & 4 \end{pmatrix} \equiv 3\begin{pmatrix} 1 & 23 \\ 19 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 69 \\ 57 & 12 \end{pmatrix} \equiv \begin{pmatrix} 3 & 17 \\ 5 & 12 \end{pmatrix} \pmod{26}.$$

We finally multiply each of our ciphertext digrams by K^{-1} to get our plaintext:

$$K^{-1}[\texttt{WG}] = \begin{pmatrix} 3 & 17 \\ 5 & 12 \end{pmatrix}\begin{pmatrix} 22 \\ 6 \end{pmatrix} = \begin{pmatrix} 312 \\ 136 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \texttt{MA},$$

$$K^{-1}[\texttt{TK}] = \begin{pmatrix} 3 & 17 \\ 5 & 12 \end{pmatrix}\begin{pmatrix} 19 \\ 10 \end{pmatrix} = \begin{pmatrix} 107 \\ 130 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \end{pmatrix} = \texttt{TH}.$$

Mapping these vectors back to their digrams, we get the plaintext `MATH`.

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.*

To show that the function represented by the fifth S-box in DES is not linear, we recall a function $f : \mathbb{Z}_2^6 \to \mathbb{Z}_2^4$ is linear if and only if for all inputs $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^6$ and for all scalars $a, b \in \mathbb{Z}_2$:

$$f(a\mathbf{x} \oplus b\mathbf{y}) = af(\mathbf{x}) \oplus bf(\mathbf{y}).$$

In particular, since we are working over $\mathbb{Z}_2$, we simply require that:

$$f(\mathbf{x} \oplus \mathbf{y}) = f(\mathbf{x}) \oplus f(\mathbf{y}) \ \forall \mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^6.$$

We now test this condition for specific inputs using the S_5-box lookup table in DES. Consider two simple input values:

$$\mathbf{x} = 000000_2, \quad \mathbf{y} = 111111_2.$$

We will first compute the sum of their separate f outputs and then we'll compare this result to the f output of their sum. Looking up their corresponding outputs in $\mathbb{Z}$ from the S_5-box table:

$$S_5(000000_2) = 0010_2, \quad S_5(111111_2) = 0001_2$$

which, when added together, results in 0011_2. If we are to evaluate S_5 again with the input $\mathbf{x} \oplus \mathbf{y}$:

$$S_5(111111_2) = 0001_2.$$

Since $0011_2 \neq 0001_2$, the function fails the linearity condition, proving that S_5 is not a linear function.

More generally, DES S-boxes are specifically designed to be non-linear to provide confusion and resist linear cryptanalysis. If they were linear, DES encryption would be significantly weaker, as is the case with the Hill cipher.