A Representation of Chaocipher

by

Ashley Ray, B.A.

A Thesis

In

Mathematics and Statistics

Submitted to the Graduate Faculty
of Texas Tech University in
Partial Fulfillment of
the Requirements for the Degree of

Master of Science

Approved

Dr. Chris Monico
Committee Chair

Dr. Clyde Martin

Peggy Gordon Miller
Dean of the Graduate School

August, 2012

TABLE OF CONTENTS

# CHAPTER 1
# BACKGROUND

## 1.1 History of Chaocipher

The inventor of Chaocipher, John F. Byrne, reveals the history of his creation in *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland*. The last chapter of the autobiography focuses on the story of Byrne's unsuccessful forty year quest to launch Chaocipher into the world for universal use. John F. Byrne had been somewhat interested in the idea of an indecipherable cipher for many years, but it was not until he read a detective story from a magazine that Byrne set out to create a cipher of his own. In this story, the hero claimed that deciphering a message was little trouble because "all such communications yield to methodic and scientific analysis" [2]. Byrne thought that, certainly, this statement couldn't possibly be true. Surely a cipher could be created that could not be broken. Byrne knew that true cryptanalysts would argue that any code could be broken and was a bit astounded that even Edgar Allen Poe, a student of cryptography, stated that "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve" [2]. Byrne, like many cryptographers, took this statement as a challenge and created his own cipher, a small device inside a cigar box and named it Chaocipher. Byrne was fully confident in the strength of his cipher and described his vision for its use:

> I envisioned, for instance, the utilization of my method and machine by business men for business communications, and by brotherhoods and social and religious institutions . . . I had, and still have in mind the universal use of my machine and method by husband, wife, or lover. My machine would be on hire, as typewriting machines now are, in hotels, steamships, and, maybe even on trains and airliners, available for anyone anywhere and at any time. And I believe, too, that the time will come–and come soon–when my system will be used in the publication of pamphlets and books written in cipher which will be unreadable except by those who are specially initiated. [2]

Byrne also claimed that his device and his principle were simple enough to be used by "any normal ten-year-old school child" and yet, he boldly stated that "if every person on earth were to encipher the same message . . . no two of the resultant encipherments would be alike" [2]. Byrne first presented his device to Marcellus Bailey, a famous patent attorney in Washington in June of 1919. Bailey, while intrigued by Chaocipher, told Byrne that he needed to have professional, detailed blueprints of his device in order to receive a patent and described the cigar box device as "scarcely more than a toy" [2]. Undaunted, Byrne worked with a first-rate draftsman for six months and returned to Bailey in 1920 with blueprints for the construction of Chaocipher. While Bailey thought the drawings were impressive, Byrne found that he was unable to find any machine makers willing to even attempt building his machine. Many machine makers refused to even give Byrne a bid, and others said that building the device would cost at least $5,000 and possibly up to $20,000 [2]. Byrne invested thousands of dollars and years of his life into making Chaocipher a success only to be rejected at every turn, which he found to be very frustrating considering that he thought the Chaocipher could be mass-produced and then sold at the price of ten dollars per device.

From 1918 until his death in 1960, Byrne continually attempted to market his cipher machine to the U.S. Government as well as to commercial industries. Among Byrne's papers donated to the National Cryptologic Museum are "four decades of correspondence between Byrne and, inter alia, the White House, the State Department, the War Department, the Attorney General's Office, the Department of Justice, and the Navy Bureau of Engineering" [4]. Further, Byrne wrote personal appeals to President and Mrs. Franklin Roosevelt, General Douglas MacArthur, William Friedman, Colonel Parker Hitt, and a "host of other high-ranking U.S. officials" [4]. Colonel Parker Hitt showed great interest in Chaocipher, but he suggested that Byrne pursue commercial use rather than governmental use of the device. Byrne also received rejection letters from *Collier's Weekly*, *Saturday Evening Post*, Bell Laboratories and the Teletype corporation. The Navy Department showed interest in Chaocipher, and on December 7, 1937, Byrne received a letter from Captain J.M. Irish, Assistant to the Chief of the Bureau of Engineering stating that "the Bureau would be very pleased to examine fully a

detailed description of your general system and of the mechanical means used for obtaining the cipher" [2]. Byrne continued to correspond with the Navy Department in the ongoing months until he went to a preliminary conference in 1938, which as he writes, "ended before it began" [2]. Commander Tucker advised Byrne to take his device to the War Department and State Department. Thus, the vicious cycle continued and Byrne presented his device again and again, never to be used by the government, nor the public.

One of Byrne's last efforts to draw attention to his cipher was his autobiography, *Silent Years*, which was published in 1953. While the book was supposedly written to tell the story of Byrne's friendship with James Joyce, the last chapter, which details the history of Chaocipher, comprises fully one eighth of the entire book [3] and "concludes with 23 pages of corresponding plaintext and ciphertext" along with a challenge to solve the remaining enciphered passages. Byrne offered a $5,000 reward or "the total royalties of the first three months after publication of the book" to the first person to come forward with the correct solution. Byrne even sent a copy of his book to Albert Einstein, along with a letter in which he wrote, "there are a few subjects in it, especially the chapter on Chaocipher, which might be of scientific interest to the Institute for Advanced Studies at Princeton"[1].

Byrne includes four exhibits of Chaocipher, the first of which is the longest and is also the exhibit Byrne prepared for his presentation to the Navy Department. This exhibit is titled "Chaocipher-The Ultimate Elusion," and the first four pages encrypt the following line repeatedly:

ALLGO OD,QU ICKBR OWNFO XESJU MPOVE RLAZY DOGTO SAVET HEIRP ARTY.

Note that this sentence uses every letter of the alphabet at least once. Byrne uses the letter Q to represent the comma and the letter W to represent the period. Lines 101-105 on the fifth page give an introduction to the Declaration of Independence and the Gettysburg Speech which are quoted from lines 105 through 248. Byrne writes that he omitted 35 characters from the Gettysburg Speech; following the omission is "a comma followed by the words 'but it can never forget what they did here' " [2]. Lines 101-105 were left to decrypt as part of the challenge (and have been deciphered in recent years as will be discussed later).

The second exhibit is comprised of four passages from the first three chapters of Caesar's *De Bello Gallico*, with the plaintext in Latin, not an English translation. Byrne chose this text because Latin does not use the letter W at all, and yet, W is frequent in the ciphertext. Further, K is also repeated frequently throughout the ciphertext despite the fact that the letter K is quite rare in the Latin language and in the chosen Latin plaintext. The second exhibit, therefore, is a good example illustrating Byrne's opinion that Chaocipher could be used in any language used by anyone in the world.

Byrne writes of the third exhibit that it "speaks for itself, and will, I fancy, be of some interest to a certain person in Washington" [2]. While the certain person in Washington remains unnamed, Byrne did address many people in Washington about his cipher over the years, and from his autobiography, it is clear that he was extremely disappointed and unimpressed with a reply from Washington in 1921 when he wrote a letter to Secretary Hughes at the State Department suggesting the use of Chaocipher. All Byrne received was a reply from the Under Secretary, Harry P. Fletcher, which read: "In reply I beg to inform you that while the Department appreciates your courtesy in bringing this matter to its attention, the codes and ciphers now used are adequate to its needs" [2]. Byrne described this reply as a "paragon of smugness," especially considering the fact that "Robert E. Sherwood was reported only a little over a year ago in all our newspapers as declaring that high Government officials, including the late Harry Hopkins, believed that the State Department code was 'very vulnerable' as far back as 1941" [2]. Byrne addresses Washington's over-confidence in it's security in his third exhibit of Chaocipher which states:

> THE HISTORY OF WAR TEEMS WITH OCCASIONS WHERE THE INTERCEPTION OF DISPATCHES AND ORDERS WRITTEN IN PLAIN LANGUAGE HAS RESULTED IN DEFEAT AND DISASTER FOR THE FORCE WHOSE INTENTIONS THUS BECAME KNOWN AT ONCE TO THE ENEMY.

The plaintext given in exhibit three is written without spaces and does not include the final "Y" at the end of the word "ENEMY." Clearly, Byrne felt that

Washington needed to be more willing to consider using ciphers posed by cryptographers rather than deem the "codes and ciphers now used" as "adequate to its needs."

The fourth and final exhibit is titled "A Glimpse of Chaos." Again, Byrne provides both plaintext and ciphertext. This exhibit is a direct quotation from a "speech made by General of the Army, Douglas MacArthur, before the joint session of Congress after his recall from Korea." Byrne also writes that this exhibit differs from the other three "in that it bears within itself full and complete instructions to an initiate for its decipherment" [2].

While these four exhibits have provided challenges for many cryptanalysts in the years since Byrne's book was published, no one came forward to claim the reward. Byrne even went so far as to challenge the American Cryptogram Association, The New York Cipher Society, William Friedman (who had rejected the usefulness of his cipher on multiple occasions) and even Professor Norbert Weiner of the Massachusetts Institute of Technology to solve his code. Byrne even suggested the cryptanalysts try to break his code with their "electronic calculating machines" [2]. Even so, Byrne's code was never broken and he died in 1960, just a few years after his autobiography was published. His son, John Byrne, Jr. took up his father's pursuit, but to no avail [4]. As Kahn writes in *The Codebreakers*,

> One may presume that the reason both for the failure of the public to read his cipher and the failure of the government to adopt it was that while the cipher probably had many merits, its many dismerits outweighed them for practical use. Byrne, like many inventors, both won and lost. His cipher was never broken. But his dream never came true. [3]

J.F. Byrne and John Byrne, Jr. kept much of the workings of Chaocipher a secret. As a result, very little was known about the Chaocipher principle until 2010 when J.F. Byrne's daughter-in-law, Mrs. Patricia Byrne, negotiated with the National Cryptologic Museum and donated J.F. Byrne's and John Byrne Jr.'s work, along with a collection of notes, correspondences, and a crude mockup of the device. Since 2010, the Chaocipher algorithm is now available to researchers, and cryptanalysts are making substantial progress in deciphering the exhibits [4].

## 1.2 The Chaocipher Algorithm

The majority of the material in this section is based on Moshe Rubin's article, "Chaocipher Revealed: The Algorithm" [5]. Byrne built his first model of the Chaocipher device inside a cigar box. The device consists of two wheels which are placed side by side and are connected so that when one wheel rotates in the clockwise direction, the other wheel rotates in the counter-clockwise direction, very similar to gears which "engage" and "disengage" (see Figure 1 below). On the outer rim of each of the two wheels are 26 moveable tiles, each one labeled with a different letter of the alphabet. In this way, there is an entire alphabet on each of the wheels. Both of the alphabets are permuted differently, so that on the left wheel we have one alphabet, with each of the 26 letters in a certain order, and on the right wheel, there is another alphabet, with each of the 26 letters in a different order. For this reason, we commonly will refer to the permuted alphabets on the left and right wheels as the left alphabet and right alphabet, respectively. At the point where the two wheels touch, one letter on the left wheel lines up with one letter on the right wheel. If we want to encrypt say, the letter 'B', we rotate the wheels so that the letter 'B' on the right wheel is at the center meeting point between the wheels. The letter which is now next to the 'B' on the left wheel is the encrypted letter. We summarize this process by emphasizing that we locate the plaintext in the right alphabet, and thereby the corresponding ciphertext in the left alphabet. After the encryption of each letter, both alphabets are permuted in a certain manner before locating the next plaintext character in the right alphabet, followed by the ciphertext in the left alphabet.

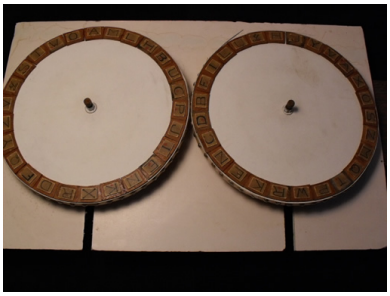

Figure 1: A wooden mockup of the Chaocipher device
(Courtesy of National Cryptologic Museum)[4]

Rubin summarizes the steps of encrypting a sequence of letters as follows:

1. Locate the next plaintext letter in the sequence to be encrypted in the right alphabet, and then use its position to locate the corresponding ciphertext letter in the left alphabet.

2. Permute the left alphabet.

3. Permute the right alphabet.

4. Repeat Steps 1-3 until all plaintext is encrypted.

As Rubin explains, the permutations are much easier to understand if we think of the left and right alphabets as 26 letter strings, rather than thinking of them in the circular format. For example, starting with the alphabets from [5]:

```
LEFT (ct):   HXUCZVAMDSLKPEFJRIGTWOBNYQ
RIGHT (pt):  PTLNBQDEOYSFAVZKGJRIHWXUMC
```

If we want to encrypt the letter `S`, we locate the letter `S` in the right alphabet. `S` is in the 11th position, so we look directly above the `S`, and we find the letter `L` in the left alphabet in the 11th position. Therefore, plaintext `S` is encrypted as ciphertext `L`.

Our next step is to permute the alphabets. The ways in which the left and right alphabets are permuted before determining the next ciphertext letter are crucial to the Chaocipher algorithm. Byrne uses the first position and the fourteenth position in his algorithm frequently, and as a result, he refers to these positions by specific names. The first position is named the *zenith*, and the fourteenth position is named the *nadir*.

To permute the left alphabet:

1. Shift the entire left alphabet cyclically to the left so that the ciphertext letter just obtained is in the first position.

2. Remove the letter in the second position, temporarily leaving an empty space in the left alphabet.

3. Shift the remaining letters from the third position up to and including the letter in the 14th position to the left, thereby filling the empty space created in the previous step. At the conclusion of this step, there should now be an empty space in the 14th position.

4. Place the removed letter from Step 2 in the fourteenth position.

For example, above we used the following left alphabet:

```
LEFT (ct):   HXUCZVAMDSLKPEFJRIGTWOBNYQ
```

To permute the left alphabet, we first shift the entire alphabet so that `L`, the ciphertext letter we just determined is in the first position:

```
LEFT (ct):   LKPEFJRIGTWOBNYQHXUCZVAMDS
```

Next, we remove the letter in the second position.

```
LEFT (ct):   L PEFJRIGTWOBNYQHXUCZVAMDS
```

Shift the letters in the third position, up to and including the letter in the 14th position, to the left, leaving an empty space in the 14th position.

```
LEFT (ct):   LPEFJRIGTWOBN YQHXUCZVAMDS
```

Insert the removed letter `K` in the 14th position.

```
LEFT (ct):   LPEFJRIGTWOBNKYQHXUCZVAMDS
```

Thus, we have the new permuted left alphabet.
To permute the right alphabet:

1. Shift the entire right alphabet cyclically to the left so that the plaintext letter just enciphered is in the first position.

2. Shift the entire right alphabet cyclically one more position to the left, thereby moving a new letter to the first position.

3. Remove the letter in the third position, temporarily leaving an empty space in the right alphabet.

4. Shift the remaining letters from the 4th position up to, and including the letter in the 14th position to the left, thereby filling the empty space created in the previous step. At the conclusion of this step, there should now be an empty space in the 14th position.

5. Place the removed letter from Step 3 in the 14th position.

Continuing our example, above we used the following right alphabet:

```
RIGHT (pt):  PTLNBQDEOYSFAVZKGJRIHWXUMC
```

First, shift the entire alphabet so that `S`, the letter just enciphered, is in the first position.

```
RIGHT (pt):  SFAVZKGJRIHWXUMCPTLNBQDEOY
```

Shifting to the left one more time, we have:

```
RIGHT (pt):  FAVZKGJRIHWXUMCPTLNBQDEOYS
```

Removing the letter in the third position yields:

```
RIGHT (pt):  FA ZKGJRIHWXUMCPTLNBQDEOYS
```

Shifting the letters in the 4th position up to and including the letter in the 14th position, we have:

```
RIGHT (pt):  FAZKGJRIHWXUM CPTLNBQDEOYS
```

Finally, inserting the removed letter in the 14th position, we get the new permuted right alphabet:

```
RIGHT (pt):  FAZKGJRIHWXUMVCPTLNBQDEOYS
```

We can now encrypt the next letter, say `E`, using these new alphabets.

```
LEFT (ct):   LPEFJRIGTWOBNKYQHXUCZVAMDS
RIGHT (pt):  FAZKGJRIHWXUMVCPTLNBQDEOYS
```

Locating `E` in the right alphabet, we see that the letter `A` is directly above `E` in the left alphabet, so the plaintext `E` is enciphered as the ciphertext `A`. From this point, we would repeat our process, permuting the left and right alphabets and enciphering the next plaintext letter, until we are finished enciphering the plaintext.

# CHAPTER 2
# CHAOCIPHER AS A SEQUENCE OF PERMUTATIONS

## 2.1 Representation in $\mathbb{Z}_{26}$

The Chaocipher algorithm explained in the previous section can be described in terms of two sequences $\sigma_n$ and $\tau_n$ of permutations on the set $\mathcal{A} = \{\texttt{A},\texttt{B},\texttt{C},\ldots,\texttt{Z}\}$ as follows. If $p_1, p_2, ...$ denotes the sequence of plaintext letters, then the ciphertext letters $c_1, c_2, ...$ are determined by $c_n = \sigma_n \tau_n^{-1}(p_n)$, where $\sigma_1$ and $\tau_1$ form the key. In terms of the Chaocipher algorithm, $\sigma_1$ represents the starting left alphabet, and $\tau_1$ represents the starting right alphabet. Further, $\sigma_{n+1}$ and $\tau_{n+1}$ (i.e., the subsequent left and right alphabets respectively) are determined from $\sigma_n$, $\tau_n$, $p_n$, and $c_n$ as follows:

Let

$$\lambda = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{BCDEFGHIJKLMNOPQRSTUVWXYZA} \end{pmatrix},$$

and let

$$\mu = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{ACDEFGHIJKLMNBOPQRSTUVWXYZ} \end{pmatrix}$$

$$\nu = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{ABDEFGHIJKLMNCOPQRSTUVWXYZ} \end{pmatrix}.$$

Then $\sigma_{n+1} = \sigma_n \lambda^{\tau_n^{-1}(p_n)-1} \mu$ and $\tau_{n+1} = \tau_n \lambda^{\tau_n^{-1}(p_n)} \nu$, where the value $\tau_n^{-1}(p_n)$ in the exponent is interpretted as an integer under the mapping $\texttt{A} \mapsto 1$, $\texttt{B} \mapsto 2$, and so on.

$\lambda$ is the permutation which shifts the entire alphabet one place to the left. By raising $\lambda$ to the appropriate power, we can shift the given alphabet the necessary number of positions to the left. This step is essential to both the left and right alphabet permutations, or by these definitions, to permutations of $\sigma$ and $\tau$ respectively. Notice that for the left alphabet permutation, we need to shift the entire alphabet to the left so that the ciphertext letter just obtained is in the first position, and for the right alphabet permutation, we need to shift the entire alphabet to the left so that the plaintext letter just enciphered is in the first

position.

$\mu$ removes the letter in the 2nd position, shifts the letters from the 3rd position up to and including the letter in the 14th position to the left and places the removed letter in the 14th position. Therefore $\mu$ is essential to the left alphabet permutation described in the previous section.

Similarly, $\nu$ removes the letter in the 3rd position, shifts the letters from the 4th position up to and including the letter in the 14th position to the left and places the removed letter in the 14th position. Therefore $\nu$ is essential to the right alphabet permutation described in the previous section.

**Example 1:** Suppose that the plaintext is SECRET and the key is given by

$$\sigma_1 = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{HXUCZVAMDSLKPEFJRIGTWOBNYQ} \end{pmatrix}$$

and

$$\tau_1 = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{PTLNBQDEOYSFAVZKGJRIHWXUMC} \end{pmatrix}.$$

Then with $p_1 = \texttt{S}$ we have

$$c_1 = \sigma_1\tau_1^{-1}(\texttt{S}) = \sigma_1(\texttt{K}) = \texttt{L}.$$

Note that we had the same result when using Byrne's algorithm above. The plaintext S becomes the ciphertext L.

We then find $\sigma_2$ and $\tau_2$ as described above:

$$\sigma_2 = \sigma_1\lambda^{\tau_1^{-1}(p_1)-1}\mu.$$

Since $\tau_1^{-1}(p_1) = \tau_1^{-1}(\texttt{S}) = \texttt{K} \mapsto 11$, we have

$$\sigma_2 = \sigma_1\lambda^{11-1}\mu = \sigma_1\lambda^{10}\mu.$$

Since multiplication of cyclic permutations is defined to be composition, we work

our way from right to left:

$$\sigma_2 = \sigma_1 \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{KLMNOPQRSTUVWXYZABCDEFGHIJ} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{ACDEFGHIJKLMNBOPQRSTUVWXYZ} \end{pmatrix}.$$

So performing the composition, we have:

$$\sigma_2 = \sigma_1 \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{KMNOPQRSTUVWXLYZABCDEFGHIJ} \end{pmatrix}.$$

Finally, writing out $\sigma_1$, we have:

$$\begin{aligned} \sigma_2 &= \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{HXUCZVAMDSLKPEFJRIGTWOBNYQ} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{KMNOPQRSTUVWXLYZABCDEFGHIJ} \end{pmatrix} \\ &= \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{LPEFJRIGTWOBNKYQHXUCZVAMDS} \end{pmatrix}. \end{aligned}$$

This result matches our result for the second left alphabet above.
We now find the second right alphabet $\tau_2$ using our formula: $\tau_2 = \tau_1 \lambda^{\tau_1^{-1}(p_1)} \nu$.
Again, $\tau_1^{-1}(p_1) = \tau_1^{-1}(\texttt{S}) = \texttt{K} \mapsto 11$, so $\tau_2 = \tau_1 \lambda^{11} \nu$.
Working from right to left, we have:

$$\begin{aligned} \tau_2 &= \tau_1 \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{LMNOPQRSTUVWXYZABCDEFGHIJK} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{ABDEFGHIJKLMNCOPQRSTUVWXYZ} \end{pmatrix} \\ &= \tau_1 \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{LMOPQRSTUVWXYNZABCDEFGHIJK} \end{pmatrix} \\ &= \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{PTLNBQDEOYSFAVZKGJRIHWXUMC} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{LMOPQRSTUVWXYNZABCDEFGHIJK} \end{pmatrix} \\ &= \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{FAZKGJRIHWXUMVCPTLNBQDEOYS} \end{pmatrix}. \end{aligned}$$

Thus, using the permutation representations, we have found $\sigma_2$ and $\tau_2$:

$$\sigma_2 = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{LPEFJRIGTWOBNKYQHXUCZVAMDS} \end{pmatrix},$$

$$\tau_2 = \begin{pmatrix} \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ \texttt{FAZKGJRIHWXUMVCPTLNBQDEOYS} \end{pmatrix}.$$

And the ciphertext $c_2$ for $p_2 = \texttt{E}$, by the formula above is $c_2 = \sigma_2\tau_2^{-1}(p_2)$.

So we get $c_2 = \sigma_2\tau_2^{-1}(\texttt{E}) = \sigma_2(\texttt{W}) = \texttt{A}$. Thus $c_2 = \texttt{A}$.

We continue this process until we have finished enciphering the word SECRET.

## 2.2 Representation in $\mathbb{Z}_6$

In this section, we consider a version of the Chaocipher algorithm modified to work on the the alphabet $\mathcal{A}_6 = \texttt{\{A,B,C,D,E,F\}}$ rather than over the full alphabet. We then describe a *known plaintext attack* on this modified algorithm. The same attack is applicable to the proper Chaocipher algorithm, but the smaller alphabet size permits a complete example to be worked out. To account for the smaller alphabet size, we will analyze the permutations in $\mathbb{Z}_6$ rather than $\mathbb{Z}_{26}$.

Keeping the same labeling and structure, but applying the principle to the alphabet $\mathcal{A}_6 = \texttt{\{A,B,C,D,E,F\}}$, we let

$$\lambda = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BCDEFA} \end{pmatrix}.$$

Note that $\lambda$ performs the same operation as before by shifting every letter to the left cyclically one time.

Also, we let

$$\mu = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{ACDBEF} \end{pmatrix},$$

and

$$\nu = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{ABDCEF} \end{pmatrix}.$$

.

Note that in $\mathbb{Z}_{26}$, $\mu$ moved the second letter to the 14th position. Since there are 26 letters in the alphabet, position 14 is 1 position past the halfway point. Here we apply the same idea to a string of length 6. The halfway point is position 3, and 1 more position to the right is position 4. So to model $\mu$ in $\mathbb{Z}_6$, we move the second letter to position 4. Similarly, in $\mathbb{Z}_{26}$, $\nu$ moved the third letter to position 14, so in $\mathbb{Z}_6$, we instead move the third letter to position 4.

Our sequences of permutations representing the left and right alphabets remain exactly the same: $\sigma_{n+1} = \sigma_n \lambda^{\tau_n^{-1}(p_n)-1}\mu \text{and} \tau_{n+1} = \tau_n \lambda^{\tau_n^{-1}(p_n)}\nu$, where the value $\tau_n^{-1}(p_n)$ in the exponent is interpretted as an integer under the mapping $\texttt{A} \mapsto 1$, $\texttt{B} \mapsto 2$ and so on. The determination of ciphertext letters also remains the same, $c_n = \sigma_n \tau_n^{-1}(p_n)$.

Since we are only using the letters `A-F`, our plaintext will resemble a string of letters rather than words, but the process is still the same.

**Example 2:** Suppose the plaintext is `FACADEBDA`, and suppose

$$\sigma_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BADFCE} \end{pmatrix},$$

and

$$\tau_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{CFADEB} \end{pmatrix}.$$

To encipher the plaintext, start with the first letter $p_1 = \texttt{F}$.

$$c_1 = \sigma_1 \tau_1^{-1}(p_1) = \sigma_1 \tau_1^{-1}(\texttt{F}) = \sigma_1(\texttt{B}) = \texttt{A}.$$

To find $\sigma_2$, we use the sequence:

$$\sigma_2 = \sigma_1 \lambda^{\tau_1^{-1}(p_1)-1}\mu = \sigma_1 \lambda^{\tau_1^{-1}(\texttt{F})-1}\mu = \sigma_1 \lambda^{2-1}\mu = \sigma_1 \lambda \mu.$$

So we have:

$$\begin{aligned}\sigma_2 &= \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BADFCE} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BCDEFA} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{ACDBEF} \end{pmatrix} \\ &= \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{AFCDEB} \end{pmatrix}.\end{aligned}$$

Similarly, to find $\tau_2$, we use the sequence:

$$\tau_2 = \tau_1 \lambda^{\tau_1^{-1}(p_1)-1} \nu = \sigma_1 \lambda^{\tau_1^{-1}(\texttt{F})} \nu = \sigma_1 \lambda^2 \nu.$$

So

$$\begin{aligned}\tau_2 &= \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{CFADEB} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{CDEFAB} \end{pmatrix} \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{ABDCEF} \end{pmatrix} \\ &= \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{ADBECF} \end{pmatrix}.\end{aligned}$$

To encipher $p_2 = \texttt{A}$, we use the same formula as before:

$$c_2 = \sigma_2 \tau_2^{-1}(p_2) = \sigma_2 \tau_2^{-1}(\texttt{A}) = \sigma_2(\texttt{A}) = \texttt{A}.$$

Continuing in this fashion, we get that the plaintext `FACADEBDA` is enciphered as the ciphertext `AADFEDACB`.

We will use this plaintext and ciphertext in the next chapter.

# CHAPTER 3
# KNOWN PLAINTEXT ATTACK

Suppose we are given a string of plaintext along with the corresponding string of ciphertext. Given no other information, using the following algorithm, we will be able to find a corresponding key. In this case, remember that the starting left and right alphabets $(\sigma_1, \tau_1)$ form the key for Chaocipher. We will be using the following 3 equations. Also, begin with $n \leftarrow 1$ and $\mathcal{X} \leftarrow \mathcal{A}_6 = \texttt{\{A,B,C,D,E,F\}}$.

$$c_n = \sigma_n \tau_n^{-1}(p_n), \tag{3.1}$$

$$\sigma_{n+1} = \sigma_n \lambda^{\tau_n^{-1}(p_n)-1} \mu, \tag{3.2}$$

$$\tau_{n+1} = \tau_n \lambda^{\tau_n^{-1}(p_n)} \nu. \tag{3.3}$$

1. Evaluate (3.1) at $n$ substituting the given values $p_n$ and $c_n$.

2. Choose a letter for $\tau_1^{-1}(p_n)$ from $\mathcal{X}$. We will denote the guess with the letter $m$, so $\tau_1^{-1}(p_n) = m$. This will also give that $c_n = \sigma_n(m)$ yielding one of the letter's locations in the left alphabet as well.

3. Substitute $m$ into eqns (3.2) and (3.3) evaluated at $n$. Then $\mathcal{X} \leftarrow \mathcal{X} - \{m\}$ and $n \leftarrow n + 1$.

4. Evaluate (3.1) at $n$ using the expanded expressions for $\sigma_n$ and $\tau_n$ found in Step 3.

5. Choose a letter $q \in \mathcal{X}$ for $\tau_1^{-1}(p_n)$. Then evaluate the expression found in Step 4, assuming $\tau_1^{-1}(p_n) = q$. Thus, we will find another letter's location in the left alphabet. Then $\mathcal{X} \leftarrow \mathcal{X} - \{q\}$.

6. If our results yield a contradiction (meaning that our result tells us a letter belongs in a location which is already filled by a different letter or that the resulting letter has already been used in a different location), we will repeat

Step 5 until we reach results which do not yield a contradiction. Keep track of choices made. If our results do not yield a contradiction to previous results, proceed to the next step.

7. Set $\mathcal{X} \leftarrow \mathcal{A}_6 - \{CurrentImage(\tau_1^{-1})\}$. Repeat Steps 5 through 6 until we have found $\sigma_1$ and $\tau_1$ completely.

**Example 3:** Suppose we are given the following plaintext `(pt)` and corresponding ciphertext `(ct)`, and wish to determine $\sigma_1$ and $\tau_1$.

`(pt): FACADEBDA,`

`(ct): AADFEDACB.`

*Step 1:* Evaluate (3.1) at $n = 1$ substituting the given values of $p_1$ and $c_1$ so that $c_1 = \sigma_1\tau_1^{-1}(p_1)$. We know $p_1 = \mathtt{F}$ and $c_1 = \mathtt{A}$, so we get:

$$\mathtt{A} = \sigma_1\tau_1^{-1}(\mathtt{F}) = \sigma_1(\tau_1^{-1}(\mathtt{F})).$$

*Step 2:* Guess $\tau_1^{-1}(\mathtt{F}) = \mathtt{B}$. Evaluate the expression found in Step 1 based on this assumption. Keep track of guesses.

$$\sigma_1(\mathtt{B}) = \mathtt{A}.$$

We now have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{A} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{F} \end{pmatrix}.$$

*Step 3:* Substitute $\mathtt{B} \mapsto 2$ into equations (3.2) and (3.3) evaluated at $n = 1$, so

$$\sigma_2 = \sigma_1\lambda^{2-1}\mu = \sigma_1\lambda\mu,$$

$$\tau_2 = \tau_1\lambda^2\nu.$$

*Step 4:* Evaluate (3.1) at $n = 2$ using the expanded expressions for $\sigma_2$ and $\tau_2$ found in step 3. For example,

$$\mathtt{A} = \sigma_2\tau_2^{-1}(\mathtt{A}) = \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}).$$

*Steps 5 and 6:* To evaluate this expression, we need to make a guess for $\tau_1^{-1}(\mathtt{A})$. The options are: $\tau_1^{-1}(\mathtt{A}) \in \{\mathtt{A},\mathtt{C},\mathtt{D},\mathtt{E},\mathtt{F}\}$. Try all of these options and see which, if any, lead to contradictions.
First assume $\tau_1^{-1}(\mathtt{A}) = \mathtt{A}$. Then

$$\begin{aligned}
\mathtt{A} &= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu(\mathtt{E}) \\
&= \sigma_1\lambda(\mathtt{E}) \\
&= \sigma_1(\mathtt{F}).
\end{aligned}$$

This is a contradiction to our prior result $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{A}) \neq \mathtt{A}$.
Second, assume $\tau_1^{-1}(\mathtt{A}) = \mathtt{C}$.

$$\begin{aligned}
\mathtt{A} &= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu(\mathtt{A}) \\
&= \sigma_1\lambda(\mathtt{A}) \\
&= \sigma_1(\mathtt{B}).
\end{aligned}$$

This statement is consistent with prior results, so $\tau_1^{-1}(\mathtt{A}) = \mathtt{C}$ is a possibility.

Third, assume $\tau_1^{-1}(\mathtt{A}) = \mathtt{D}$.

$$\begin{aligned}
\mathtt{A} &= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This is a contradiction to our prior result $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{A}) \neq \mathtt{D}$.
Fourth, assume $\tau_1^{-1}(\mathtt{A}) = \mathtt{E}$.

$$\begin{aligned}
\mathtt{A} &= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu(\mathtt{D}) \\
&= \sigma_1\lambda(\mathtt{B}) \\
&= \sigma_1(\mathtt{C}).
\end{aligned}$$

This is a contradiction to our prior result $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{A}) \neq \mathtt{E}$.
Finally, assume $\tau_1^{-1}(\mathtt{A}) = \mathtt{F}$.

$$\begin{aligned}
\mathtt{A} &= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\nu^{-1}\lambda^{-2}(\mathtt{F}) \\
&= \sigma_1\lambda\mu\nu^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{C}) \\
&= \sigma_1\lambda(\mathtt{D}) \\
&= \sigma_1(\mathtt{E}).
\end{aligned}$$

This is a contradiction to our prior result $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{A}) \neq \mathtt{F}$.

Therefore, if Step 1 is correct, then $\tau_1^{-1}(\mathtt{A}) = \mathtt{C}$ and we have $\sigma_1(\mathtt{B}) = \mathtt{A}$.

Noting our progress, we have:

$$\sigma_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{A} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{FA} \end{pmatrix}.$$

*Step 7:* Repeat process until both $\sigma_1$ and $\tau_1$ are found.

Evaluating (3.2) and (3.3) at $n = 2$ we get:

$$\sigma_3 = \sigma_2 \lambda^{\tau_2^{-1}(\texttt{A})-1} \mu,$$

$$\tau_3 = \tau_2 \lambda^{\tau_2^{-1}(\texttt{A})} \nu.$$

To simplify these expressions we need to evaluate $\tau_2^{-1}(\texttt{A})$ in the exponent.

$$\begin{aligned} \tau_2^{-1}(\texttt{A}) &= \nu^{-1}\lambda^{-2}\tau_1^{-1}(\texttt{A}) \\ &= \nu^{-1}\lambda^{-2}(\texttt{C}) \\ &= \nu^{-1}(\texttt{A}) \\ &= \texttt{A} \mapsto 1. \end{aligned}$$

Also, we will replace $\sigma_2$ and $\tau_2$ with the equivalent expanded expressions found previously. We have the following:

$$\sigma_3 = \sigma_1 \lambda\mu\lambda^{1-1}\mu = \sigma_1 \lambda\mu\mu,$$

$$\tau_3 = \tau_1 \lambda^2\nu\lambda^1\nu = \tau_1 \lambda^2\nu\lambda\nu.$$

Evaluating (3.1) at $n = 3$, we have $\texttt{D} = \sigma_3\tau_3^{-1}(\texttt{C})$.
Replacing $\sigma_3$ and $\tau_3^{-1}$ using the equivalent expanded expressions above,

$$\texttt{D} = \sigma_1 \lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\texttt{C})$$

To evaluate this expression we need to make a guess as to what $\tau_1^{-1}(\texttt{C})$ is. The remaining options are: $\tau_1^{-1}(\texttt{C}) \in \{\texttt{A,D,E,F}\}$. Try all of the options to see if any lead to contradictions and determine which are possibilities.

First, assume $\tau_1^{-1}(\mathtt{C}) = \mathtt{A}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{C}) \\
&= \sigma_1\lambda\mu(\mathtt{D}) \\
&= \sigma_1\lambda(\mathtt{B}) \\
&= \sigma_1(\mathtt{C}).
\end{aligned}$$

This result does not contradict previous results, so $\tau_1^{-1}(\mathtt{C}) = \mathtt{A}$ could be a possibility. Second, assume $\tau_1^{-1}(\mathtt{C}) = \mathtt{D}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{A}) \\
&= \sigma_1\lambda\mu(\mathtt{A}) \\
&= \sigma_1\lambda(\mathtt{A}) \\
&= \sigma_1(\mathtt{B}).
\end{aligned}$$

This is a contradiction to our prior result $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{C}) \neq \mathtt{D}$.

Third, assume $\tau_1^{-1}(\mathtt{C}) = \mathtt{E}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This result does not contradict previous results, so $\tau_1^{-1}(\mathtt{C}) = \mathtt{E}$ could be a possibility. Finally, assume $\tau_1^{-1}(\mathtt{C}) = \mathtt{F}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}\lambda^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This result does not contradict previous results, so $\tau_1^{-1}(\mathtt{C}) = \mathtt{F}$ could be a possibility. So $\tau_1^{-1}(\mathtt{C}) \in \{\mathtt{A},\mathtt{E},\mathtt{F}\}$.
First, we will try $\tau_1^{-1}(\mathtt{C}) = \mathtt{A}$. If this leads to a contradiction in future steps, we will come back to this step and try one of the other two possibilities.

Now if $\tau_1^{-1}(\mathtt{C}) = \mathtt{A}$, then we also know $\sigma_1(\mathtt{C}) = \mathtt{D}$. So we have the following:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{AD} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFA} \end{pmatrix}.$$

Evaluating (3.2) and (3.3) at $n = 3$, we repeat the necessary computations as before to get:

$$\sigma_4 = \sigma_3 \lambda^{\tau_3^{-1}(\mathtt{C})-1} \mu,$$

$$\tau_4 = \tau_3 \lambda^{\tau_3^{-1}(\mathtt{C})} \nu.$$

For both equations, we need to find $\tau_3^{-1}(\mathtt{C})$.

$$\begin{aligned} \tau_3^{-1}(\mathtt{C}) &= \nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{C}) \\ &= \nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{A}) \\ &= \nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{E}) \\ &= \nu^{-1}\lambda^{-1}(\mathtt{E}) \\ &= \nu^{-1}(\mathtt{D}) \\ &= \mathtt{C} \mapsto 3. \end{aligned}$$

So substituting this value for $\tau_3^{-1}(\mathtt{C})$ yields:

$$\sigma_4 = \sigma_3 \lambda^{3-1} \mu,$$

$$\tau_4 = \tau_3 \lambda^3 \nu.$$

And replacing $\sigma_3$ and $\tau_3$ with their equivalent expanded expressions yields:

$$\sigma_4 = \sigma_1 \lambda \mu \mu \lambda^2 \mu,$$

$$\tau_4 = \tau_1 \lambda^2 \nu \lambda \nu \lambda^3 \nu.$$

Now we can evaluate equation (3.1) at $n = 4$.

$$\begin{aligned}
\mathtt{F} &= \sigma_4\tau_4^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{F}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}\lambda^{-3}(\mathtt{F}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This statement does not contradict previous results, so we continue to the next step.

Noting our progress, we now have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{ADF} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFA} \end{pmatrix}.$$

Evaluating (3.2) and (3.3) at $n = 4$, we repeat the necessary computations as before.

$$\sigma_5 = \sigma_4\lambda^{\tau_4^{-1}(\mathtt{A})-1}\mu,$$

$$\tau_5 = \tau_4\lambda^{\tau_4^{-1}(\mathtt{A})}\nu.$$

For both equations, we need to find $\tau_4^{-1}(\mathtt{A})$.

$$\begin{aligned}
\tau_4^{-1}(\mathtt{A}) &= \nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{A}) \\
&= \nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{C}) \\
&= \nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{A}) \\
&= \nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{A}) \\
&= \nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{F}) \\
&= \nu^{-1}\lambda^{-3}(\mathtt{F}) \\
&= \nu^{-1}(\mathtt{C}) \\
&= (\mathtt{D}) \mapsto 4.
\end{aligned}$$

So substituting this value for $\tau_4^{-1}(\mathtt{A})$ yields:

$$\sigma_5 = \sigma_4\lambda^{4-1}\mu,$$

$$\tau_5 = \tau_4\lambda^4\nu.$$

And replacing $\sigma_4$ and $\tau_4$ with their equivalent expanded expressions yields:

$$\sigma_5 = \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu,$$

$$\tau_5 = \tau_1\lambda^2\nu\lambda\nu\lambda^3\nu\lambda^4\nu.$$

Evaluating (3.1) at $n = 5$ yields:

$$\begin{aligned}
\mathtt{E} &= \sigma_5\tau_5^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{D}).
\end{aligned}$$

To complete this computation, we need to figure out what $\tau_1^{-1}(\mathtt{D})$ is. We have 3 remaining options to check: $\tau_1^{-1}(\mathtt{D}) \in \{\mathtt{D},\mathtt{E},\mathtt{F}\}$.

First, assume $\tau_1^{-1}(\mathtt{D}) = \mathtt{D}$.

$$\begin{aligned}
\mathtt{E} &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{E}) \\
&= \sigma_1\lambda\mu(\mathtt{E}) \\
&= \sigma_1\lambda(\mathtt{E}) \\
&= \sigma_1(\mathtt{F}).
\end{aligned}$$

This result is not in contradiction to previous results, so $\tau_1^{-1}(\mathtt{D}) = \mathtt{D}$ could be a possibility.

Second, assume $\tau_1^{-1}(\mathtt{D}) = \mathtt{E}$.

$$\begin{aligned}
\mathtt{E} &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{A}) \\
&= \sigma_1\lambda\mu(\mathtt{A}) \\
&= \sigma_1\lambda(\mathtt{A}) \\
&= \sigma_1(\mathtt{B}).
\end{aligned}$$

This is a contradiction to our previous result that $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{D}) \neq \mathtt{E}$.

Finally, assume $\tau_1^{-1}(\mathtt{D}) = \mathtt{F}$.

$$\begin{aligned}
\mathtt{E} &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{F}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}\lambda^{-4}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This is a contradiction to our previous result that $\sigma_1(\mathtt{B}) = \mathtt{A}$, so $\tau_1^{-1}(\mathtt{D}) \neq \mathtt{F}$.

Therefore, we know $\tau_1^{-1}(\mathtt{D}) = \mathtt{D}$, and therefore $\sigma_1(\mathtt{F}) = \mathtt{E}$. Noting our results, we have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{ADF\ E} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFAD} \end{pmatrix}.$$

Again, we evaluate (3.2) and (3.3), this time at $n = 5$.

$$\sigma_6 = \sigma_5\lambda^{\tau_5^{-1}(\mathtt{D})-1}\mu,$$

$$\tau_6 = \tau_5\lambda^{\tau_5^{-1}(\mathtt{D})}\nu.$$

To evaluate the exponents in both equations we need $\tau_5^{-1}(\mathtt{D})$.

$$\begin{aligned}
\tau_5^{-1}(\mathtt{D}) &= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{D}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{D}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{B}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{B}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{A}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{A}) \\
&= \nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{D}) \\
&= \nu^{-1}\lambda^{-4}(\mathtt{C}) \\
&= \nu^{-1}(\mathtt{E}) \\
&= \mathtt{E} \mapsto 5.
\end{aligned}$$

Now, using this value and the equivalent expanded expressions for $\sigma_5$ and $\tau_5$ we have:

$$\sigma_6 = \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu,$$

$$\tau_6 = \tau_1\lambda^2\nu\lambda\nu\lambda^3\nu\lambda^4\nu\lambda^5\nu.$$

Next, evaluating (3.1) at $n = 6$,

$$\begin{aligned}
\mathtt{D} &= \sigma_6\tau_6^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{E}).
\end{aligned}$$

Now we know $\tau_1^{-1}(\mathtt{E}) \in \{\mathtt{E},\mathtt{F}\}$. First, assume $\tau_1^{-1}(\mathtt{E}) = \mathtt{E}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{C}) \\
&= \sigma_1\lambda\mu(\mathtt{D}) \\
&= \sigma_1\lambda(\mathtt{B}) \\
&= \sigma_1(\mathtt{C}).
\end{aligned}$$

This result does not contradict previous results, so $\tau_1^{-1}(\mathtt{E}) = \mathtt{E}$ is a possibility.

Next, consider $\tau_1^{-1}(\mathtt{E}) = \mathtt{F}$.

$$\begin{aligned}
\mathtt{D} &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}(\mathtt{F}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}(\mathtt{E}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}\lambda^{-5}(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\nu^{-1}(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4(\mathtt{C}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3(\mathtt{A}) \\
&= \sigma_1\lambda\mu\mu\lambda^2\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu\mu\lambda^2(\mathtt{B}) \\
&= \sigma_1\lambda\mu\mu(\mathtt{D}) \\
&= \sigma_1\lambda\mu(\mathtt{B}) \\
&= \sigma_1\lambda(\mathtt{C}) \\
&= \sigma_1(\mathtt{D}).
\end{aligned}$$

This is a contradiction to our previous result $\sigma_1(\mathtt{D}) = \mathtt{F}$.

Therefore, our only possibility is $\tau_1^{-1}(\mathtt{E}) = \mathtt{E}$, so we also have $\mathtt{D} = \sigma_1(\mathtt{C})$.

Keeping track of our results, we now have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{ADF\ E} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFADE} \end{pmatrix}.$$

Again, we evaluate (3.2) and (3.3), this time at $n = 6$.

$$\sigma_7 = \sigma_6 \lambda^{\tau_6^{-1}(\mathtt{E})-1} \mu,$$

$$\tau_7 = \tau_6 \lambda^{\tau_6^{-1}(\mathtt{E})} \nu.$$

Calculating using the same process as in previous steps, we find that $\tau_6^{-1}(\mathtt{E}) = \mathtt{E} \mapsto 5$.

After replacing $\sigma_6$ and $\tau_6$ with their respective expanded expressions, we have the following:

$$\sigma_7 = \sigma_1 \lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu,$$

$$\tau_7 = \tau_1 \lambda^2\nu\lambda\nu\lambda^3\nu\lambda^4\nu\lambda^5\nu\lambda^5\nu.$$

Then, we evaluate (3.1) again at $n = 7$ to get:

$$\begin{aligned} \mathtt{A} &= \sigma_7\tau_7^{-1}(\mathtt{B}) \\ &= \sigma_1 \lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{B}). \end{aligned}$$

Our only remaining option for $\tau_1^{-1}(\mathtt{B})$ is $\mathtt{F}$. Working from right to left and evaluating as before, we find that $\mathtt{A} = \sigma_1(\mathtt{B})$, which affirms prior results.

Noting these results, we now have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{ADF\ E} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFADEB} \end{pmatrix}.$$

We have now completed the starting right alphabet, $\tau_1$. We still lack two letters positions in $\sigma_1$. We know $\mathtt{B}$ and $\mathtt{C}$ belong in the two remaining positions, but we don't know which place exactly. At this point, we could use trial and error. For example, we could suppose $\sigma_1(\mathtt{A}) = \mathtt{B}$ and $\sigma_1(\mathtt{E}) = \mathtt{C}$. Then we can test to see if this is correct. If not, we know that $\mathtt{B}$ and $\mathtt{C}$ must switch places. Even so, we want to show that the sequences of permutations presented in this paper may be used to directly find $\sigma_1$ and $\tau_1$, so we will continue our process the necessary two steps further.

Continuing, evaluate (3.2) and (3.3) at $n = 7$.

$$\sigma_8 = \sigma_7 \lambda^{\tau_7^{-1}(\mathtt{B})-1} \mu,$$

$$\tau_8 = \tau_7 \lambda^{\tau_7^{-1}(\mathtt{B})} \nu.$$

Evaluating as before, we find that $\tau_7^{-1}(\mathtt{B}) = \mathtt{D} \mapsto 4$.

Note that replacing $\sigma_7$ and $\tau_7$ with their respective expanded expressions yields:

$$\sigma_8 = \sigma_1 \lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu\lambda^3\mu,$$

$$\tau_8 = \tau_1 \lambda^2\nu\lambda\nu\lambda^3\nu\lambda^4\nu\lambda^5\nu\lambda^5\nu\lambda^4\nu.$$

Then evaluating (3.1) at $n = 8$, we have:

$$\begin{aligned} \mathtt{C} &= \sigma_8 \tau_8^{-1}(\mathtt{D}) \\ &= \sigma_1 \lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\mathtt{D}). \end{aligned}$$

Computing from right to left as before, we get that $\mathtt{C} = \sigma_1(\mathtt{E})$.

We now have:

$$\sigma_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{ADFCE} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \mathtt{ABCDEF} \\ \mathtt{CFADEB} \end{pmatrix}.$$

Finally, evaluate (3.2) and (3.3) at $n = 8$.

$$\sigma_9 = \sigma_8 \lambda^{\tau_8^{-1}(\mathtt{D})-1} \mu,$$

$$\tau_9 = \tau_8 \lambda^{\tau_8^{-1}(\mathtt{D})} \nu.$$

Computing, we find that $\tau_8^{-1}(\mathtt{D}) = \mathtt{D} \mapsto 4$. Replacing $\sigma_9$ and $\tau_9$ with their respective expanded expressions yields:

$$\sigma_9 = \sigma_1 \lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu\lambda^3\mu\lambda^3\mu,$$

$$\tau_9 = \tau_1 \lambda^2\nu\lambda\nu\lambda^3\nu\lambda^4\nu\lambda^5\nu\lambda^5\nu\lambda^4\nu\lambda^4\nu.$$

Evaluating (3.1) at $n = 9$ yields:

$$\begin{aligned}\texttt{B} &= \sigma_9\tau_9^{-1}(\texttt{A}) \\ &= \sigma_1\lambda\mu\mu\lambda^2\mu\lambda^3\mu\lambda^4\mu\lambda^4\mu\lambda^3\mu\lambda^3\mu\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-5}\nu^{-1}\lambda^{-4}\nu^{-1}\lambda^{-3}\nu^{-1}\lambda^{-1}\nu^{-1}\lambda^{-2}\tau_1^{-1}(\texttt{A}).\end{aligned}$$

Computing from right to left as before, we find that $\texttt{B} = \sigma_1(\texttt{A})$.

Finally, we have both $\sigma_1$ and $\tau_1$.

$$\sigma_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BADFCE} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{CFADEB} \end{pmatrix}.$$

Notice that these two alphabets are the exact same alphabets we used in Chapter 2 to encrypt the plaintext we used in this example.

**Remark** : As seen in the example, the equations used become progressively longer with every step. For this reason, it is helpful to look at these equations in smaller pieces in order to shorten the calculations. Each time we evaluate (3.1) and substitute the expanded expressions for $\sigma_n, \tau_n$ found in the previous step, we get an equation of the form:

$$c_n = \sigma_1 ... \tau_1^{-1}(p_n)$$

The sequence of permutations between $\sigma_1$ and $\tau_1^{-1}(p_n)$ in any such equation can be written as a composition of two permutations $\alpha_n, \beta_n$ defined such that

$$\alpha_1 = \lambda^{\tau_1^{-1}(p_1)-1}\mu$$

$$\beta_1 = \nu^{-1}\lambda^{-\tau_1^{-1}(p_1)}.$$

And for $n \geq 1$,

$$\alpha_{n+1} = \alpha_n\lambda^{\tau_n^{-1}(p_n)-1}\mu$$

$$\beta_{n+1} = \nu^{-1}\lambda^{-\tau_n^{-1}(p_n)}\beta_n.$$

In this way, our expanded expressions may be computed more quickly, and for $n \geq 1$, we have:

$$c_{n+1} = \sigma_1\alpha_n\beta_n\tau_1^{-1}(p_{n+1}).$$

Further, it should also be noted that there are five other possible starting alphabets. If for our first guess in Step 2, we say that $\tau_1^{-1}(\texttt{F}) = \texttt{C}$, for example, and

repeat the entire process, our resulting $\sigma_1$ and $\tau_1$ are as follows:

$$\sigma_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{EBADFC} \end{pmatrix} \quad \text{and} \quad \tau_1 = \begin{pmatrix} \texttt{ABCDEF} \\ \texttt{BCFADE} \end{pmatrix}.$$

Notice that if we compare these alphabets, the letters are in the exact same order as before. The only difference is that in the second set of alphabets, each letter is shifted cyclically to the right one position. The first guess will determine the starting place for the same cycle of letters. This means that there are at least six possible starting left and right alphabets for any given piece of plaintext and corresponding ciphertext.

The analogous statement holds in $\mathbb{Z}_{26}$. There are at least 26 possible starting alphabets for any given plaintext and corresponding ciphertext, and the exact same permutation sequences will lead the cryptanalyst to a key. Of course, the computations in $\mathbb{Z}_{26}$ would take quite a long time to do by hand, but with the help of a computer, we should be able to apply the same algorithm to any plaintext and ciphertext encrypted using Chaocipher, as long as the known plaintext and ciphertext both contain all 26 letters of the alphabet.

From the example shown here, we see that a string of 7 plaintext letters along with the corresponding ciphertext were sufficient to find $\tau_1$, but not $\sigma_1$. To find $\sigma_1$ completely, we need a known plaintext size of length 9. Notice that if we look back at the given plaintext and ciphertext, we see that once we reach $p_7$, every letter in $\mathcal{A}_6$ appears at least once. Since we use $\tau_1$ to locate plaintext, it makes sense that we were able to find all of $\tau_1$ after 7 operations. The ciphertext string, however, still had not used letters `B` and `C`, so we did not have enough information to completely determine $\sigma_1$ after 7 operations. It is not until we reach $c_9$ that every letter in $\mathcal{A}_6$ has appeared at least once in the given ciphertext. For this reason, in this particular example, we needed a known-plaintext size of length 9, and it took 9 operations to find $\sigma_1$ and $\tau_1$ completely.

We can then estimate that the known-plaintext size required depends upon the letters present in a given string. We will be able to determine a key if all letters in $\mathcal{A}_6$ appear once in both the plaintext and the ciphertext. Further work will need to be done to determine an estimate of this size. Also, it would be interesting to

determine how many operations, on average, would be needed to determine a key using this known-plaintext attack.

# BIBLIOGRAPHY

[1] Chaocipher-related material. http://www.mountainvistasoft.com/chaocipher/Silent-Years-Chapter-21-Chaocipher.pdf, 2012.

[2] John F. Byrne. *Silent Years: An Autobiography with Memoirs of James Joyce and Our Ireland*. Farrar, Straus Young, New York, 1953.

[3] David Kahn. *The Codebreakers*. Scribner, New York, 1967.

[4] National Cryptologic Museum. Chaocipher machine and papers. http://www.cryptologicfoundation.org/content/Direct-Museum-Support/recentacquisitions.shtml#Chaocipher, 2012.

[5] Moshe Rubin. Chaocipher revealed: The algorithm. Chaocipher Clearing House, http://www.mountainvistasoft.com/chaocipher/.