Classical Substitution Ciphers and Group Theory

Thomas Kaeding
insanitas@proton.me

spring, 2023

We explore some connections between classical substitution ciphers, both monoalphabetic and polyalphabetic, and mathematical group theory. We try to do this in a way that is accessible to cryptographers who are not familiar with group theory, and to mathematicians who are not familiar with classical ciphers.

Introduction

This article explores some of the connections between classical substitution ciphers and mathematical group theory. The ciphers that concern us are both monoalphabetic (i.e., always making the same substitution whenever the same letter is encountered) and polyalphabetic (using a collection of monoalphabetic substitutions in some determined order). It is our hope that the material presented here is understandable both to amateur cryptographers who have never studied modern algebra, and to mathematicians who have no familiarity with classical ciphers. The goal is to acquire the ability to use some concepts of group theory to help in understanding the analysis of the ciphers.

The ciphers that we consider are well explained in [1] and [2]. An introduction to modern algebra, including group theory, can be found in many textbooks, such as [3]. We will not, however, assume that the reader is familiar with any of these materials. Many of the ideas presented here are in a much more compact and obtuse format in a short series of articles [4]. Modular arithmetic and its connection to some ciphers are also treated in [5] and [6].

Groups

In order to understand what we mean by "group," we have first to discuss sets and operators. A *set* is simply a collection of things. Those things can be numbers, letters, email addresses, mathematical functions, or even other sets. The things in a set are its *elements*. To say that some thing x is in a set S, we often use a symbol, like this: $x \in S$. Two very important sets for us are the set of integers, which we denote with a fancy $\mathbb{Z}$:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

and the alphabet of 26 letters:

{A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z}

Later on, we will be looking at subsets of $\mathbb{Z}$ and sets comprised of cipher keys.

Now that we have sets, we need to know what to do with them. A *binary operator* is a prescription for taking two things and giving back a third. Addition (+), subtraction (−), and multiplication (· or ×) are familiar binary operators on numbers. Division (÷ or ⁄), however, is not, since we cannot divide by zero. When we are not sure of the nature of a binary operator, we can denote it by some other symbol, such as ▪ or ◇ or ★.

We are now ready to define a group. A *group* is a set S with a binary operator • such that

1. the set S is *closed* under the binary operator, i.e., for every x and y in S, $x \bullet y$ is also in S;

2. the binary operator is *associative*:

$$(x \bullet y) \bullet z \;=\; x \bullet (y \bullet z)$$

for every x, y, z in S;

3. S contains an *identity element* e such that

$$x \bullet e \;=\; e \bullet x \;=\; x$$

for every x in S;

4. every x in S has an *inverse* y, such that

$$x \bullet y \;=\; y \bullet x \;=\; e$$

When we talk about groups, we usually write a set with its binary operator as a doublet, like this: $(S, \bullet)$. The idea of closure may seem obvious, but we need to mention it to exclude such possibilities as the inner vector product. The inner vector product, also called the dot product, takes two vectors and returns a scalar (just a number); so the set of vectors is not closed under this operation. The associative property is another one that we usually assume holds; in this article we will not see any examples in which it does not.

Be aware that we did not include the *commutative* property. An operator is *commutative* if for every x and y in the set,

$$x \bullet y \;=\; y \bullet x$$

If a group's operation is commutative, we say that the group is *commutative* or *abelian*. Otherwise, we call it *noncommutative* or *nonabelian*. In general, a group is not commutative, so be careful not to make an assumption that it is.

A quick example may make things clearer. $(\mathbb{Z}, +)$ is a group. Clearly, if we take any two integers m and n, then $m + n$ is also an integer (closure). Also, for any three integers,

$$(k + m) + n \;=\; k + (m + n)$$

so we have associativity. The identity element e is zero (0):

$$0 + n \;=\; n + 0 \;=\; n$$

for any n in $\mathbb{Z}$. And the inverse of any n is simply $-n$:

$$n + (-n) \;=\; (-n) + n \;=\; 0$$

Finally, we note that $(\mathbb{Z}, +)$ is a commutative group, since

$$m + n \;=\; n + m$$

for any integers m and n.

Now let us think about a counterexample. $(\mathbb{Z}, \cdot)$ is *not* a group. It is closed, since the product of any two integers is also an integer. It is associative. It has an identity element: one (1). But where it fails is in the lack of inverses. There is no integer n such that

$$3 \cdot n \;=\; n \cdot 3 \;=\; 1$$

for example. In other words, 3^{-1} is not in the set of integers.

With addition, we will usually write inverses as $-x$, as we did above with $(\mathbb{Z}, +)$. For any other binary operator, we will usually write the inverse of x as x^{-1}, as we do for multiplication.

To help us get accustomed to thinking abstractly, let us consider a group of emojis. Take the set

$\mathcal{E}$ = {☺, ☹, ⚇}

and define a binary operator ✶ by its “multiplication table”:

✶	☺	☹	⚇
☺	☹	⚇	☺
☹	⚇	☺	☹
⚇	☺	☹	⚇

Closure of ($\mathcal{E}$, ✶) is obvious. If we check, we will find that we have associativity and commutivity. The identity element is ⚇:

⚇ ✶ ⚇ = ⚇
⚇ ✶ ☺ = ☺ ✶ ⚇ = ☺
⚇ ✶ ☹ = ☹ ✶ ⚇ = ☹

The symbols ☺ and ☹ are inverses of each other:

☺ ✶ ☹ = ☹ ✶ ☺ = ⚇

The Caesar shift cipher and modular addition

The first cipher we want to consider is one of the simplest: the *Caesar shift cipher*. The key for this cipher is an integer from 0 to 25 (although 0 results in no encryption). To encrypt a text, we merely shift each letter along the alphabet to the right by the number of steps given by the key. If we run off the end of the alphabet, we wrap around to the beginning. For example, if the key is 7, then A → H, B → I, C → J, ..., Y → F, Z → G. Decryption is the inverse process.

One useful way to think about this cipher, especially if we are writing computer programs to implement it, is to assign an integer to each of the letters: A = 0, B = 1, ..., Z = 25. The action of the cipher is to add the key to each of these integers, with one twist: if the sum is ever larger than 25, then we subtract 26 to bring it back into the range 0, 1, ..., 25. Addition with this new property is called *modular addition*, and we say that we are adding numbers *modulo* 26. The number 26 is the *modulus*. We can think of it as identifying the modulus with zero, i.e., 26 = 0. To decrypt, we subtract the key, again with the twist that if we get a result outside the range, we must adjust it. For subtraction, we must add 26 to bring us back in. Now let us think about this in the context of groups.

The group ($\mathbb{Z}_{26}$, + mod 26)

Let us consider the set of integers that are used in the Caesar shift cipher. It is a subset of the integers ranging from 0 to 25. Since the modulus for this subset is 26, we denote it as $\mathbb{Z}_{26}$:

$$\mathbb{Z}_{26} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}$$

On this set we are defining a binary operation that is addition modulo 26, where if the result is ever outside of the set, we subtract 26 until we get a number in it. So, for example,

$$15 + 18 = 33 \rightarrow 7$$

In this new way of adding, we simply write

$$15 + 18 = 7$$

I made a table for addition modulo 26, so now you have to look at it:

+ mod 26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
2	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1
3	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2
4	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3
5	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4
6	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5
7	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6
8	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7
9	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8
10	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9
11	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10
12	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12
14	14	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13
15	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
16	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
17	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
18	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
19	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
20	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
21	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
22	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
23	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
24	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
25	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

The set $\mathbb{Z}_{26}$ with addition modulo 26 is a group. Closure is guaranteed by the way that we defined modular addition. Associativity is present, although we will not prove it. The identity element is zero (0), as we would expect. But now we have to think of inverses differently that with regular addition. We can write the inverse of n as $-n$, but keep in mind that negative numbers are *not* in the set. What we call "−5," for example, is actually 21, since

$$5 + 21 \;=\; 21 + 5 \;=\; 0$$

modulo 26. Thus, the inverse of 5 is 21.

This group has more structure hidden in it. To see it, we first define the order of an element. Its *order* is the smallest number of times we combine that element with itself using the binary operation of the group so that the result is the identity element. For this group, the operation is a form of addition, so the order is the smallest number of times we must add an element to get 0. For example, the order of 4 is 13, since

$$4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 \;=\; 0$$

in addition modulo 26 (in regular addition, the result is 52, but $52 - 26 - 26 = 0$). Here is a table of the elements of $\mathbb{Z}_{26}$ and their orders:

element(s)	order
0	1
13	2
2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	13
1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25	26

Now, $26 = 2 \cdot 13$. Notice that if an element shares one of these factors, its order is reduced by that factor. We say that ($\mathbb{Z}_{26}$, + mod 26) is a *cyclic* group, because it contains at least one element whose order is the same as the size of the set. Because of this feature, an order-26 element is able to *generate* the whole group by successive operations using that element. Such an element is called a *generator*. For example, 1 is obviously a generator, since we can obtain any element in the set by adding some 1's. Less obvious is 9. By adding 9's, we can also generate the group:

$$\begin{aligned} 9 &= 9 \\ 9+9 &= 18 \\ 9+9+9 &= 1 \\ 9+9+9+9 &= 10 \\ 9+9+9+9+9 &= 19 \\ 9+9+9+9+9+9 &= 2 \\ &\ldots \end{aligned}$$

If we check, we will find that the *orbit* of 9 reaches every element in the set before coming to 0.

The orbit of 13 has only two elements: 0 and 13. In this way, 13 generates a cyclic two-element subgroup, ({0, 13}, + mod 26). In a similar manner, any of the order-13 elements generates a cyclic subgroup with thirteen elements, ({0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24}, + mod 26).

This might be a good time to introduce the idea of isomorphism. An isomorphism is a mapping from one group to another, such that every element in the first group is mapped to exactly one element in the second group, every element in the second group is mapped from an element in the first, and the structure of the binary operation is the same. That last condition can be expressed as follows: Suppose the two groups are (S, ▪) and (T, ◇). An isomorphism is a map $\varphi\colon S \rightarrow T$ such that

$$\varphi\,(x \blacksquare y) \;=\; \varphi\,(x) \diamond \varphi\,(y)$$

for any x and y in S. Notice that the binary operation ▪ is for S, and ◇ is for T. With an isomorphism, it does not matter if we operate before (in S with ▪) or after mapping (in T with ◇). When two groups are isomorphic, we write

$$(S, \blacksquare) \;\cong\; (T, \diamond)$$

The subgroup generated by any of the even-numbered elements of $\mathbb{Z}_{26}$ is isomorphic to the group using addition modulo 13:

$$(\{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24\}, + \text{ mod } 26) \;\cong\; (\mathbb{Z}_{13}, + \text{ mod } 13)$$

One possible mapping is the obvious one:

$$\begin{aligned} 0 &\to 0 \\ 2 &\to 1 \\ 4 &\to 2 \\ &\cdots \end{aligned}$$

However, there are eleven other mappings that also work, such as

$$\begin{aligned} 0 &\to 0 \\ 4 &\to 1 \\ 8 &\to 2 \\ &\cdots \\ 2 &\to 7 \\ 6 &\to 8 \\ &\cdots \end{aligned}$$

The other subgroup of ($\mathbb{Z}_{26}$, + mod 26) is isomorphic to a group with addition modulo 2:

$$(\{0, 13\}, + \bmod 26) \cong (\mathbb{Z}_2, + \bmod 2)$$

There is only one mapping for this isomorphism:

$$\begin{aligned} 0 &\to 0 \\ 13 &\to 1 \end{aligned}$$

An isomorphism from a group to itself is called an *automorphism*. What are the automorphisms of ($\mathbb{Z}_{26}$, + mod 26)? Suppose we multiply every element by 5, and keep the convention of subtracting 26 until the result is back in $\mathbb{Z}_{26}$. This is an automorphism:

$$5\,(x + y) = 5x + 5y$$

The same argument works for multiplication by any of the order-26 element of ($\mathbb{Z}_{26}$, + mod 26). However, it fails for any element that shares a factor with 26. For example, if we multiply every element by 13, we find that for half of them we obtain 0, which is a violation of the rule that the mapping of an isomorphism takes only one element to an element in the target. This motivates us to examine the set of order-26 elements, and we shall do so below.

The multiplication cipher

Suppose now that we employ a cipher in which the letters are not shifted by a constant, but are multiplied by the key number [5]. Like before, we assign numbers 0, ..., 25 to the letters, as A = 0, B = 1, ..., Z = 25. We must keep the convention that if the result of the multiplication exceeds 26, then we subtract 26 repeatedly until we are in the range 0, ..., 25. If the key is 7, for example, then during encryption

$$\begin{aligned} A &= 0 \rightarrow 0 = A \\ B &= 1 \rightarrow 7 = H \\ C &= 2 \rightarrow 14 = O \\ &\dots \\ Z &= 25 \rightarrow 19 = T \end{aligned}$$

We must now consider whether every multiplier is acceptable for this cipher. If $k = 0$, clearly the result is always 0 = A, and the cipher becomes useless. If k is even, then we have the problem that only even-numbered letters can appear in the ciphertext. Decrypting cannot unambiguously be done in this case. And if $k = 13$, the ciphertext is a series of As and Ns. The rule is that the key may not share a factor with 26 = 2·13. The set of acceptable multipliers has a name, $\mathbb{Z}_{26}^*$, and it is the set of all integers that have an inverse under multiplication modulo 26. More on it below.

The group ($\mathbb{Z}_{26}^*$, · mod 26)

The binary operation that concerns us here is multiplication modulo 26. It is worth repeating that this means that any time we multiply two elements of $\mathbb{Z}_{26}$, if the result is greater than 26, then we must subtract 26 repeatedly until the result fall within the range 0, ..., 25. The relevant question is which elements have an inverse under multiplication modulo 26. To get a handle on this question, let us build the multiplication table:

· mod 26	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
8	0	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18
9	0	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17
10	0	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16
11	0	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15
12	0	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14
13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13
14	0	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12
15	0	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11
16	0	16	6	22	12	2	18	8	01	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10
17	0	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9
18	0	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8
19	0	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7
20	0	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6

21	0	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5
22	0	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4
23	0	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3
24	0	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2
25	0	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

As expected, 1 is the identity element for multiplication, as we can see in the row or column for 1. However, 1 only appears twelve times in the bulk of the table. The rows (or columns) in which it appears are those for which an inverse exists. For example, $7 \cdot 15 = 1$, so 7 has an inverse, which is 15. The invertible elements form a special set:

$$\mathbb{Z}_{26}^{*} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

These are the elements of $\mathbb{Z}_{26}$ that are *coprime* to the modulus 26, i.e., they do not share any prime factors with the modulus.

Together with multiplication modulo 26, this set forms a group. To see that it is closed, we can take the table and remove the rows and columns for the numbers not in the set:

· mod 26	1	3	5	7	9	11	15	17	19	21	23	25
1	1	3	5	7	9	11	15	17	19	21	23	25
3	3	9	15	21	1	7	19	25	5	11	17	23
5	5	15	25	9	19	3	23	7	17	1	11	21
7	7	21	9	23	11	25	1	15	3	17	5	19
9	9	1	19	11	3	21	5	23	15	7	25	17
11	11	7	3	25	21	17	9	5	1	23	19	15
15	15	19	23	1	5	9	17	21	25	3	7	11
17	17	25	7	15	23	5	21	3	11	19	1	9
19	19	5	17	3	15	1	25	11	23	9	21	7
21	21	11	1	17	7	23	3	19	9	25	15	5
23	23	17	11	5	25	19	7	1	21	15	9	3
25	25	23	21	19	17	15	11	9	7	5	3	1

Since only the elements of $\mathbb{Z}_{26}^{*}$ appear in the table, we have closure. It is associative, but we will not prove it. From the symmetry of the multiplication table about the main diagonal, we know that this group is commutative. The identify element, as we noted above, is 1, and every element in $\mathbb{Z}_{26}^{*}$ has an inverse. In general, whenever we have an additive group $\mathbb{Z}_{m}$ with modulus m, then the set of elements that are coprime with the modulus is called $\mathbb{Z}_{m}^{*}$, and with multiplication modulo m it forms its own group.

Finally, we want to note that the elements of $\mathbb{Z}_{26}^{*}$ are the automorphisms of $\mathbb{Z}_{26}$. We can see in the full 26×26 multiplication table, that those rows corresponding to the elements of $\mathbb{Z}_{26}^{*}$ contain all twenty-six numbers 0, 1, ..., 25. And, without checking every possibility, we state that for any a in $\mathbb{Z}_{26}^{*}$ and any x and y in $\mathbb{Z}_{26}$, we can define the automorphism by

$$\varphi(x) = a \cdot x$$

so that

$$\varphi\,(x + y) \;=\; a \cdot (x + y) \;=\; (a \cdot x) + (a \cdot y) \;=\; \varphi\,(x) + \varphi\,(y)$$

where all of the multiplications and additions are performed modulo 26.

By the way, $(\mathbb{Z}_{26}^{*}, \cdot \bmod 26)$ is isomorphic to $(\mathbb{Z}_{12}, + \bmod 12)$. One of several such mappings is

$$\begin{array}{rcrcr@{\qquad\qquad}rcrcr}
7^0 & = & 1 & \rightarrow & 0 & 7^6 & = & 25 & \rightarrow & 6 \\
7^1 & = & 7 & \rightarrow & 1 & 7^7 & = & 19 & \rightarrow & 7 \\
7^2 & = & 23 & \rightarrow & 2 & 7^8 & = & 3 & \rightarrow & 8 \\
7^3 & = & 5 & \rightarrow & 3 & 7^9 & = & 21 & \rightarrow & 9 \\
7^4 & = & 9 & \rightarrow & 4 & 7^{10} & = & 17 & \rightarrow & 10 \\
7^5 & = & 11 & \rightarrow & 5 & 7^{11} & = & 15 & \rightarrow & 11
\end{array}$$

The other possibilities involve powers of 11, 15, and 19.

General monoalphabetic substitution cipher

We saw the Caesar shift cipher and the multiplication cipher, but their keyspaces are very small. So now we move on to the general monoalphabetic substitution cipher. Here, the key is a rearrangement (a permutation) of the alphabet. Letters of the plaintext are replaced by their corresponding letters in the key. For example, if our key is

$$k \;=\; \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

then letters are replaced as follows:

$$\begin{array}{ll}
\text{plaintext:} & \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\
 & \downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow\downarrow \\
\text{ciphertext:} & \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}
\end{array}$$

We will sometimes write the substitution cipher as a function S, and write the encryption process that takes plaintext P to ciphertext C as

$$C \;=\; S\,(k, P)$$

The decryption process is the inverse function:

$$P \;=\; S^{-1}\,(k, C)$$

The group of permutations

There are 26! permutations of the twenty-six letters; let us put them into a set and call it Π. How can we take two of these permutations and combine them? The most reasonable approach for an amateur cryptographer is to consider the two permutations k_1 and k_2 as keys for the substitution cipher, and encrypt a text twice:

$$S\,(k_2, S\,(k_1, P))$$

We can then think of the final output as having resulted from a single equivalent key k_3:

$$S\,(k_2, S\,(k_1, P)) \;=\; S\,(k_3, P)$$

This operation we call *composition*, and we write it like this:

$$k_3 \;=\; k_2 \circ k_1$$

Notice that the first key is on the right, and the second is to its left. This is the normal way in which mathematicians write things, since things usually act on other things to the right.

A quick example shows how we can find the composition of two permutations. Consider our key from above:

$$k_1 \;=\; \mathtt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

A second key can be chosen as

$$k_2 \;=\; \mathtt{SPACEFLIGHTZYXWVURQONMKJDB}$$

It is helpful to write out how letters are replaced using these permutations:

```
plaintext:     ABCDEFGHIJKLMNOPQRSTUVWXYZ
               ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:    FLYINGSAUCERBDHJKMOPQTVWXZ

plaintext:     ABCDEFGHIJKLMNOPQRSTUVWXYZ
               ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:    SPACEFLIGHTZYXWVURQONMKJDB
```

The combined key must take, for example, `M` to `B` when the first permutation acts, and then that `B` becomes `P` under the action of the second permutation; so `M` → `P` in the composition. When we trace through each of the twenty-six letters, we find

```
plaintext:     ABCDEFGHIJKLMNOPQRSTUVWXYZ
               ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:    FZDGXLQSNAERPCIHTYWVUOMKJB
```

Thus, the composition is

$$k_3 \;=\; k_2 \circ k_1 \;=\; \mathtt{FZDGXLQSNAERPCIHTYWVUOMKJB}$$

Composition of this sort is a binary operation on the set Π. This operation is associative: for all x, y, and z in Π,

$$(x \circ y) \circ z = x \circ (y \circ z)$$

For this reason, we will often drop parentheses and simply write this combination as $x \circ y \circ z$. Be careful, however, because this operation is *not* commutative; in general,

$$x \circ y \neq y \circ x$$

There is a special permutation that does not change any of the letters. It is the identity element in Π, and we call it e:

$$e = \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$$

Can we find the inverse of a permutation? Of course, we can. In terms of the substitution cipher, the inverse of a key is the key that is used to decrypt a text:

$$P = S^{-1}(k, C) = S(k^{-1}, C)$$

For example, let us take the permutation we used above:

$$k = \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

The inverse of this key does the opposite, so we write its action with upward arrows:

$$\begin{array}{ll} \text{plaintext:} & \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\ & \uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow \\ \text{ciphertext:} & \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ} \end{array}$$

Next we take the columns are rearrange them so that the bottom row is the straight alphabet. The upper row is then the inverse permutation:

$$\begin{array}{ll} \text{plaintext:} & \texttt{HMJNKAFODPQBRESTULGVIWXYCZ} \\ & \uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow \\ \text{ciphertext:} & \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \end{array}$$

$$k^{-1} = \texttt{HMJNKAFODPQBRESTULGVIWXYCZ}$$

The reader can check that

$$k^{-1} \circ k = k \circ k^{-1} = e$$

Putting it all together, we see that $(\Pi, \circ)$ is a noncommutative group. The binary operation is the composition of permutations, there is an identity element, and every permutation has an inverse.

Cycles

Every permutation can be factored into a product of disjoint cycles. A *cycle* is permutation that cycles through some letters; it permutes them as though they were attached to a wheel. Letters that do not participate in the cycle remain fixed. So, for example, the cycle (ADG) takes A → D, D → G, and G → A, and all other letters remain themselves. (Notice the special notation for a cycle. Also note that we can write this one as (DGA) or (GAD).)

Let us see how to factor a permutation into cycles with an example. Recall our favorite key:

$$k = \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

and remember that it acts on letters as follows:

plaintext:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
	↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:	FLYINGSAUCERBDHJKMOPQTVWXZ

If we start with A, we see that it is replaced by F. But F is replaced by G, and G by S, etc. When the chain comes back around to A, we have found the complete cycle:

$$\texttt{A} \to \texttt{F} \to \texttt{G} \to \texttt{S} \to \texttt{O} \to \texttt{H} \to \texttt{A}$$

Thus, *k* has (AFGSOH) as a factor. If we start new chains on letters that we have not used already, and continue the process, then will find that *k* has these five cycles:

$$k = (\texttt{AFGSOH})\,(\texttt{BLRM})\,(\texttt{CYXWVTPJ})\,(\texttt{DIUQKEN})\,(\texttt{Z})$$

In this notation, we leave out the ◦ symbol. Notice that the last cycle (a 1-cycle) does nothing; it takes Z to itself. We call these cycles *disjoint* because they do not share any letters. A cycle involving *n* letters, and therefore having order *n*, is called an *n-cycle*.

The order of a cycle is the number of letters that participate in it. In our example, the cycle (AFGSOH) has six letters, and therefore has order 6. Thus, the composition of six of them gives the identity permutation:

$$(\texttt{AFGSOH}) \circ (\texttt{AFGSOH}) \circ (\texttt{AFGSOH}) \circ (\texttt{AFGSOH}) \circ (\texttt{AFGSOH}) \circ (\texttt{AFGSOH}) = e$$

When a permutation is factored into disjoint cycles, the order of the permutation is the least common multiple (lcm) of the orders of the cycles. For our example, then,

$$\mathrm{ord}\,(k) = \mathrm{lcm}\,(6, 4, 8, 7, 1) = 168$$

and

$$k^{168} = e$$

The inverse of a cycle is simply written in reverse order. It does not matter on which letter we begin the cycle, so for our example, the inverse of (AFGSOH) can be written (HOSGFA) or (AHOSGF) or one of four other ways. The inverse of a permutation that has been factored into cycles can be written as the product of the inverse cycles. For our example,

$$k^{-1} = \text{(AHOSGF) (BMRL) (CJPTVWXY) (DNEKQUI) (Z)}$$

The Vigenère cipher

The *Vigenère cipher* [1] [2] [7] is a polyalphabetic substitution and is usually described using the following tableau. The key is a word or phrase, and the encryptor cycles repeatedly through the key as the text is encrypted. For a given plaintext letter and a given key letter, the ciphertext letter is found on the row of the tableau corresponding to the key letter and in the column corresponding to the plaintext letter. For example, if the plaintext letter is E and the key letter is J, then the ciphertext letter is N.

shift key	plaintext letters	label of
letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ	permutation
A	ABCDEFGHIJKLMNOPQRSTUVWXYZ	$R_0 = e$
B	BCDEFGHIJKLMNOPQRSTUVWXYZA	R_1
C	CDEFGHIJKLMNOPQRSTUVWXYZAB	R_2
D	DEFGHIJKLMNOPQRSTUVWXYZABC	R_3
E	EFGHIJKLMNOPQRSTUVWXYZABCD	R_4
F	FGHIJKLMNOPQRSTUVWXYZABCDE	R_5
G	GHIJKLMNOPQRSTUVWXYZABCDEF	R_6
H	HIJKLMNOPQRSTUVWXYZABCDEFG	R_7
I	IJKLMNOPQRSTUVWXYZABCDEFGH	R_8
J	JKLMNOPQRSTUVWXYZABCDEFGHI	R_9
K	KLMNOPQRSTUVWXYZABCDEFGHIJ	R_{10}
L	LMNOPQRSTUVWXYZABCDEFGHIJK	R_{11}
M	MNOPQRSTUVWXYZABCDEFGHIJKL	R_{12}
N	NOPQRSTUVWXYZABCDEFGHIJKLM	R_{13}
O	OPQRSTUVWXYZABCDEFGHIJKLMN	R_{14}
P	PQRSTUVWXYZABCDEFGHIJKLMNO	R_{15}
Q	QRSTUVWXYZABCDEFGHIJKLMNOP	R_{16}
R	RSTUVWXYZABCDEFGHIJKLMNOPQ	R_{17}
S	STUVWXYZABCDEFGHIJKLMNOPQR	R_{18}
T	TUVWXYZABCDEFGHIJKLMNOPQRS	R_{19}
U	UVWXYZABCDEFGHIJKLMNOPQRST	R_{20}
V	VWXYZABCDEFGHIJKLMNOPQRSTU	R_{21}
W	WXYZABCDEFGHIJKLMNOPQRSTUV	R_{22}
X	XYZABCDEFGHIJKLMNOPQRSTUVW	R_{23}
Y	YZABCDEFGHIJKLMNOPQRSTUVWX	R_{24}
Z	ZABCDEFGHIJKLMNOPQRSTUVWXY	R_{25}

To be sure that we understand this cipher, let us work an example. Suppose that our plaintext is

```
LAUNCHFROMSPACEPORTSEVEN
```

and that our key is ALIEN. We make as many copies of the key as we need to encrypt the entire text. For each letter of the text, we look for the letter in the table at the intersection of its column with the row specified by the key letter. The column of the first letter, L, meets the row of the first key letter, A, at L. The column of the second letter, A, meets the row of the second key letter, L, also at L. The column of the third letter, U, meets the row of the third key letter, I, at C. We continue in this fashion until the entire text is encrypted.

plaintext:	LAUNCHFROMSPACEPORTSEVEN
key:	ALIENALIENALIENALIENALIE
ciphertext:	LLCRPHQZSZSAIGRPZZXFEGMR

Another way to implement the cipher is to work with numerical values. Again, we can assign A = 0, B = 1, ..., Z = 25. Then, if the key is a list of letters/numbers k_i for $i = 0, ..., L-1$ when the length of the key is L, and the plaintext letters are p_i for $i = 0, 1, 2, ...$, then the ciphertext letters are

$$c_i = (k_{i \bmod L} + p_i) \bmod 26$$

However, they way we want to envision the Vigenère cipher is as a periodic set of monoalphabetic substitution ciphers. And each of those monoalphabetic substitutions is a Caesar shift cipher. Earlier, we looked at the Caesar shift in terms of the numerical equivalents of the letters. But now, let us reinterpret the cipher in terms of permutations of the alphabet. For example, if the key is 7, then the permutation is

$$R_7 = \texttt{HIJKLMNOPQRSTUVWXYZABCDEFG}$$

We have decided to call it “R_7” because it is a rotation of the alphabet leftward by seven steps. In the Vigenère tableau each row is one such rotation. The rotation of zero steps is the identity permutation.

The collection of the twenty-six rotations is a set we will call

$$\mathcal{V} = \{R_n\}$$

Let us now examine how elements in this set behave under the binary operation that is composition of permutations. The composition of two rotations is another rotation,

$$R_m \circ R_n = R_{m+n}$$

where the addition in the subscript is performed modulo 26. Since $R_0 = e$, this means that each rotation has an inverse, which is

$$R_n^{-1} = R_{-n}$$

where "$-n$" in the subscript means the additive inverse of n modulo 26 (the same as $26 - n$). We have now essentially shown that $(\mathcal{V}, \circ)$ is a group.

Earlier we saw that the set of possible keys for the Caesar shift cipher was $\mathbb{Z}_{26}$. Now we claim that the Vigenère group is isomorphic to it:

$$(\mathcal{V}, \circ) \;\cong\; (\mathbb{Z}_{26}, + \bmod 26)$$

There are several (twelve) possible ways to define the mapping, but the most natural way is

$$\varphi\,(R_n) \;=\; n$$

so that

$$\varphi\,(R_m \circ R_n) \;=\; \varphi\,(R_{m+n}) \;=\; m + n \;=\; \varphi\,(R_m) + \varphi\,(R_n)$$

where all of the addition is done modulo 26. The twelve possibilities for the mapping correspond to the twelve elements of $\mathbb{Z}_{26}^{*}$; if a is such an element, then the mapping

$$\varphi\,(R_n) \;=\; a \cdot n$$

is a perfectly good isomorphism, when the multiplication is done modulo 26.

It will be useful later to know the orders of the elements of $\mathcal{V}$. Since R_0 is already the identity element, it has order 1. There is one element with order 2, and it is R_{13}. The remaining odd-numbered rotations have order 26, while all of the even-numbered rotations have order 13.

It will also be useful later to know the factorization into cycles for the elements of $\mathcal{V}$. It is tedious but not difficult for the reader to work them out. We will merely tabulate the results:

elements	order	cycles
R_0	1	26 1-cycles
R_{13}	2	13 2-cycles
$R_2, R_4, R_6, R_8, R_{10}, R_{12}, R_{14}, R_{16}, R_{18}, R_{20}, R_{22}, R_{24}$	13	2 13-cycles
$R_1, R_3, R_5, R_7, R_9, R_{11}, R_{15}, R_{17}, R_{19}, R_{21}, R_{23}, R_{25}$	26	1 26-cycle

The multiplication cipher, revisited

Earlier we looked at the multiplication cipher in terms of numbers and multiplication modulo 26. But like the Caesar shift cipher, we can instead find alphabetic permutations to represent the action of the cipher. Here we list those permutations for the valid choices of the multiplier:

M_1 = `ABCDEFGHIJKLMNOPQRSTUVWXYZ` = e
M_3 = `ADGJMPSVYBEHKNQTWZCFILORUX`
M_5 = `AFKPUZEJOTYDINSXCHMRWBGLQV`

$$\begin{aligned}
M_7 &= \texttt{AHOVCJQXELSZGNUBIPWDKRYFMT}\\
M_9 &= \texttt{AJSBKTCLUDMVENWFOXGPYHQZIR}\\
M_{11} &= \texttt{ALWHSDOZKVGRCNYJUFQBMXITEP}\\
M_{15} &= \texttt{APETIXMBQFUJYNCRGVKZODSHWL}\\
M_{17} &= \texttt{ARIZQHYPGXOFWNEVMDULCTKBSJ}\\
M_{19} &= \texttt{ATMFYRKDWPIBUNGZSLEXQJCVOH}\\
M_{21} &= \texttt{AVQLGBWRMHCXSNIDYTOJEZUPKF}\\
M_{23} &= \texttt{AXUROLIFCZWTQNKHEBYVSPMJGD}\\
M_{25} &= \texttt{AZYXWVUTSRQPONMLKJIHGFEDCB}
\end{aligned}$$

We can put these twelve permutations into a set which we call $\mathcal{M}$. Like $\mathcal{V}$, it is a subset of the full set of permutations of the alphabet, Π. This new set is closed under composition of permutations:

$$M_m \circ M_n \;=\; M_{m \cdot n}$$

where the multiplication in the subscript is done modulo 26. We can see that the identity element $e = M_1$ is a member of the set. What is less obvious is that the inverse of each M_n in also in the set. The reader can easily verify that

$$\begin{aligned}
M_1^{-1} &= M_1\\
M_3^{-1} &= M_9\\
M_5^{-1} &= M_{21}\\
M_7^{-1} &= M_{15}\\
M_{11}^{-1} &= M_{19}\\
M_{17}^{-1} &= M_{23}\\
M_{25}^{-1} &= M_{25}
\end{aligned}$$

Notice that M_1 and M_{25} are *self-reciprocal* (also called *involutory*), and that M_{25} takes the role of -1 (modulo 26) in this system. Another way to express the inverse of M_m is

$$M_m^{-1} \;=\; M_{1/m}$$

where we have written $1/m$ in the subscript to mean m^{-1} for convenience.

We now know that $(\mathcal{M}, \circ)$ is a group, and that it is commutative. Furthermore, it is isomorphic to $(\mathbb{Z}_{26}^{*}, \cdot \bmod 26)$. The natural mapping is

$$\varphi\,(M_n) \;=\; n$$

so that

$$\varphi\,(M_m \circ M_n) \;=\; \varphi\,(M_{m \cdot n}) \;=\; m \cdot n \;=\; \varphi\,(M_m) \cdot \varphi\,(M_n)$$

where all of the multiplications are performed modulo 26.

The set $\mathcal{M}$ is the set of automorphisms of $\mathcal{V}$, just as we saw earlier that the elements of $\mathbb{Z}_{26}^{*}$ are the automorphisms of $\mathbb{Z}_{26}$. Here, however, the automorphism takes the form

$$\varphi_m(R_n) \; = \; M_m \circ R_n \circ M_m^{-1}$$

Recall that earlier we saw that an automorphism of ($\mathbb{Z}_{26}$, + mod 26) takes any element x to $a{\cdot}x$ mod 26, where a is an element of $\mathbb{Z}_{26}^*$. An automorphism on $\mathcal{V}$ does something similar. We state without proving it that

$$M_m \circ R_n \; = \; R_{m\cdot n} \circ M_m$$

where the multiplication in the subscript is performed modulo 26 (the reader can convince oneself of the truth of this statement by simply trying all 312 possibilities). Therefore,

$$\varphi_m(R_n) \; = \; M_m \circ R_n \circ M_m^{-1} \; = \; R_{m\cdot n} \circ M_m \circ M_m^{-1} \; = \; R_{m\cdot n} \circ e \; = \; R_{m\cdot n}$$

And to see that it is an automorphism,

$$\begin{aligned} \varphi_m(R_n \circ R_p) \; &= \; M_m \circ R_n \circ R_p \circ M_m^{-1} \\ &= \; M_m \circ R_n \circ e \circ R_p \circ M_m^{-1} \\ &= \; M_m \circ R_n \circ (M_m^{-1} \circ M_m) \circ R_p \circ M_m^{-1} \\ &= \; (M_m \circ R_n \circ M_m^{-1}) \circ (M_m \circ R_p \circ M_m^{-1}) \\ &= \; \varphi_m(R_n) \circ \varphi_m(R_p) \end{aligned}$$

The affine cipher

The key for an affine cipher is a pair of integers. One, say m, is from $\mathbb{Z}_{26}^*$ so that it has a multiplicative inverse, and the other, say n, is from $\mathbb{Z}_{26}$. Letters are converted to numbers in the usual way, A = 0, B = 1, ..., Z = 25, and each letter is encrypted according to the formula

$$c_i \; = \; m \cdot p_i + n$$

where all of the arithmetic is done modulo 26. Clearly, the affine cipher is equivalent to a multiplication cipher followed by a Caesar shift. Decryption must be done in the reverse order:

$$p_i \; = \; m^{-1} \cdot [c_i + (-n)]$$

If we now treat the affine cipher in terms of alphabetic permutations, then a generic key $A_{m,n}$ can be written as a composition of a multiplication from $\mathcal{M}$ and a rotation from $\mathcal{V}$:

$$A_{m,n} \; = \; R_n \circ M_m$$

Remember that the permutation on the right acts first. Next consider the set of all such keys:

$$\mathcal{A} \; = \; \{A_{m,n}\} \; = \; \{R_n \circ M_m \mid m \in \mathbb{Z}_{26}^*, n \in \mathbb{Z}_{26}\}$$

This set has 312 members, including the one that leaves the plaintext unchanged ($R_0 \circ M_1$).

Is $(\mathcal{A}, \circ)$ a group? In order to answer this question, we need to learn a bit more about how its members behave when composed with one another. In particular, we need to know how to handle $M_m \circ R_n$. First of all, we note that for any permutation π, $\pi \circ R_n$ is the rotation of π leftward by n steps. When we rotate one of the M_m by n steps, what happens? Earlier, we stated without proving that

$$M_m \circ R_n \; = \; R_{m \cdot n} \circ M_m$$

where the multiplication in the subscript is done modulo 26. If there is any doubt, there are only 312 cases that need to be checked. Now we can check for closure. Take any two keys and find their composition:

$$\begin{aligned} A_{c,d} \circ A_{a,b} \; &= \; (R_d \circ M_c) \circ (R_b \circ M_a) \\ &= \; R_d \circ (M_c \circ R_b) \circ M_a \\ &= \; R_d \circ R_{b \cdot c} \circ M_c \circ M_a \\ &= \; R_{b \cdot \mathrm{c}+d} \circ M_{a \cdot c} \\ &= \; A_{a \cdot c,\, b \cdot c+d} \end{aligned}$$

where all arithmetic in the subscripts is performed modulo 26. This agrees with what we already know about the affine cipher; here we take two sequential encryptions,

$$p_i \; \rightarrow \; a \cdot p_i + b \; \rightarrow \; c \cdot (a \cdot p_i + b) + d \; = \; (a \cdot c) \cdot p_i + (b \cdot c + d)$$

which are equivalent to one encryption with multiplier $a \cdot c$ and shift $b \cdot c + d$. The identity element is contained in the set:

$$e \; = \; M_1 \circ R_0$$

The inverse of $A_{m,n} = R_n \circ M_m$ is $M_m^{-1} \circ R_n^{-1}$:

$$M_m^{-1} \circ R_n^{-1} \circ \; R_n \circ M_m \; = \; M_m^{-1} \circ (R_n^{-1} \circ \; R_n) \circ M_m \; = \; M_m^{-1} \circ e \circ M_m \; = \; M_m^{-1} \circ M_m \; = \; e$$

but

$$M_m^{-1} \circ R_n^{-1} \; = \; M_{1/m} \circ R_{-n} \; = \; R_{-n/m} \circ \; M_{1/m}$$

where we have written $1/m$ in place of m^{-1} for convenience. Therefore,

$$A_{m,n}^{-1} \; = \; A_{1/m,-n/m}$$

i.e., the key with multiplier m^{-1} and shift $-m^{-1} \cdot n$ (all done modulo 26). This also agrees with the numerical interpretation of the affine cipher:

$$m^{-1} \cdot (m \cdot p_i + n) + m^{-1} \cdot (-n) \; = \; (m^{-1} \cdot m) \cdot p_i + m^{-1} \cdot n + m^{-1} \cdot (-n) \; = \; 1 \cdot p_i + 0 \; = \; p_i$$

We now have everything we need (assuming associativity holds) to declare that $(\mathcal{A}, \circ)$ is a group. This group is not commutative.

There is a construction in mathematics called the one-dimensional affine group. It is the set of functions

$$\{f(x) = ax + b\}$$

where a is invertible, together with composition of functions as its binary operation. If we take our coefficients from $\mathbb{Z}_{26}$, then the invertible coefficients are found in $\mathbb{Z}_{26}{}^{*}$. The group $(\mathcal{A}, \circ)$ is isomorphic to this affine group:

$$(\mathcal{A}, \circ) \;\cong\; (\{f(x) = ax + b \mid a \in \mathbb{Z}_{26}{}^{*},\, b \in \mathbb{Z}_{26}\}, \circ)$$

We pause here to make a comment about the versatility of the composition operation in the group of permutations. With the rotations of $\mathcal{V}$ we had a subgroup that was isomorphic to an additive group. The set $\mathcal{M}$ of keys for the multiplication cipher we saw was a group isomorphic to a multiplicative group. And now, we have an isomorphism to a group whose operation is the composition of functions.

Do the elements of $\mathcal{A}$ give automorphisms of $\mathcal{V}$, as did the elements of $\mathcal{M}$? Let us find out:

$$\begin{aligned}
A_{m,n} \circ R_p \circ A_{m,n}{}^{-1} &= (R_n \circ M_m) \circ R_p \circ (R_n \circ M_m)^{-1} \\
&= R_n \circ M_m \circ R_p \circ M_{1/m} \circ R_{-n} \\
&= R_n \circ R_{m \cdot p} \circ M_m \circ M_{1/m} \circ R_{-n} \\
&= R_n \circ R_{m \cdot p} \circ e \circ R_{-n} \\
&= R_n \circ R_{m \cdot p} \circ R_{-n} \\
&= R_{m \cdot p+n-n} \;=\; R_{m \cdot p}
\end{aligned}$$

where all arithmetic in the subscripts is done modulo 26. Thus,

$$A_{m,n} \circ R_p \circ A_{m,n}{}^{-1} \;=\; M_m \circ R_p \circ M_m{}^{-1}$$

and $\mathcal{A}$ contains a redundant set of automorphisms of $\mathcal{V}$.

Quagmire 1 cipher

We are now ready to move on to other polyalphabetic ciphers. We begin with the quagmire ciphers. The traditional way to envision the *quagmire 1* (Q1) is to start with the Vigenère tableau, and permute the list of plaintext letters across the top [1] [2]. For our favorite "base key," we have this table:

shift key	plaintext letters
letters	F L Y I N G S A U C E R B D H J K M O P Q T V W X Z
A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B	B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C	C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

E	E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F	F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G	G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H	H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I	I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J	J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K	K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L	L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M	M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O	O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P	P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q	Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R	R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S	S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T	T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V	V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W	W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X	X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y	Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z	Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Encryption works the same way as with the Vigenère. For example, if the plaintext letter is E and the shift key letter is S, then the ciphertext letter is C.

It should be obvious that encryption is performing an inverse monoalphabetic substitution (the permutation of the plaintext letters at the top of the tableau) followed by a Vigenère cipher. So the quagmire 1 cipher can be factored into these two ciphers [8] [9]:

$$C = Q_1 (k_{\text{alpha}}, k_{\text{shift}}, P) = V (k_{\text{shift}}, (S^{-1} (k_{\text{alpha}}, P))$$

If we straighten out the plaintext alphabet at the top of the table, for the example above, by shifting the columns, we obtain this tableau:

shift key	plaintext letters
letters	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	H M J N K A F O D P Q B R E S T U L G V I W X Y C Z
B	I N K O L B G P E Q R C S F T U V M H W J X Y Z D A
C	J O L P M C H Q F R S D T G U V W N I X K Y Z A E B
D	K P M Q N D I R G S T E U H V W X O J Y L Z A B F C
E	L Q N R O E J S H T U F V I W X Y P K Z M A B C G D
F	M R O S P F K T I U V G W J X Y Z Q L A N B C D H E
G	N S P T Q G L U J V W H X K Y Z A R M B O C D E I F
H	O T Q U R H M V K W X I Y L Z A B S N C P D E F J G

I	PURVSINWLXYJZMABCTODQEFGKH
J	QVSWTJOXMYZKANBCDUPERFGHLI
K	RWTXUKPYNZALBOCDEVQFSGHIMJ
L	SXUYVLQZOABMCPDEFWRGTHIJNK
M	TYVZWMRAPBCNDQEFGXSHUIJKOL
N	UZWAXNSBQCDOERFGHYTIVJKLPM
O	VAXBYOTCRDEPFSGHIZUJWKLMQN
P	WBYCZPUDSEFQGTHIJAVKXLMNRO
Q	XCZDAQVETFGRHUIJKBWLYMNOSP
R	YDAEBRWFUGHSIVJKLCXMZNOPTQ
S	ZEBFCSXGVHITJWKLMDYNAOPQUR
T	AFCGDTYHWIJUKXLMNEZOBPQRVS
U	BGDHEUZIXJKVLYMNOFAPCQRSWT
V	CHEIFVAJYKLWMZNOPGBQDRSTXU
W	DIFJGWBKZLMXNAOPQHCRESTUYV
X	EJGKHXCLAMNYOBPQRIDSFTUVZW
Y	FKHLIYDMBNOZPCQRSJETGUVWAX
Z	GLIMJZENCOPAQDRSTKFUHVWXBY

The first thing to notice is that, like in the original table, each column contains exactly one of each letter. For lack of a better name, we call this the "column property." Below we will find that the other quagmires share this property. Each row of the tableau above is a permutation of the alphabet. Because the action of the quagmire 1 cipher is an inverse monoalphabetic substitution followed by a Vigenère cipher, each of these permutations has the form $R_n \circ k^{-1}$. We can form a set such permutations, give a base key k:

$$Q_1[k] = \{R_n \circ k^{-1}\}$$

Mathematicians define a *coset* of a subgroup as follows. Suppose we have a group $(G, \bullet)$ and a subgroup of G that is $(S, \bullet)$. Take any element h in G that is not also in S. Then for any x in S, the product $x \bullet h$ will typically not be in S. If we collect all such products into a new set,

$$H = \{x \bullet h \mid x \in S, h \in G, h \notin S\}$$

we call it a *right coset* of S. The set H cannot be a group. For one thing, it is not closed, since typically the product $x \bullet h \bullet y \bullet h$ is not also in H. For another, the identity element e cannot be in H, since e must be S (it is a group), and for any x in S, x^{-1} is also in S, so h cannot be x^{-1}. If instead we take the products with h on the left, we call the resulting set a *left coset*.

Since each member of the set $Q_1[k]$ has the form $R_n \circ h$, where h is some fixed member of Π and is "multiplied" on the right, we say that $Q_1[k]$ is a *right coset* of $\mathcal{V}$. Below we will see that the quagmire 2 forms a left coset of $\mathcal{V}$.

Quagmire 2 cipher

To implement the *quagmire 2* (Q2) we begin with the Vigenère tableau and replace the rotated alphabets in the body of the table with shifted versions of our base key [1] [2]:

shift key letters	plaintext letters A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	A U C E R B D H J K M O P Q T V W X Z F L Y I N G S
B	B D H J K M O P Q T V W X Z F L Y I N G S A U C E R
C	C E R B D H J K M O P Q T V W X Z F L Y I N G S A U
D	D H J K M O P Q T V W X Z F L Y I N G S A U C E R B
E	E R B D H J K M O P Q T V W X Z F L Y I N G S A U C
F	F L Y I N G S A U C E R B D H J K M O P Q T V W X Z
G	G S A U C E R B D H J K M O P Q T V W X Z F L Y I N
H	H J K M O P Q T V W X Z F L Y I N G S A U C E R B D
I	I N G S A U C E R B D H J K M O P Q T V W X Z F L Y
J	J K M O P Q T V W X Z F L Y I N G S A U C E R B D H
K	K M O P Q T V W X Z F L Y I N G S A U C E R B D H J
L	L Y I N G S A U C E R B D H J K M O P Q T V W X Z F
M	M O P Q T V W X Z F L Y I N G S A U C E R B D H J K
N	N G S A U C E R B D H J K M O P Q T V W X Z F L Y I
O	O P Q T V W X Z F L Y I N G S A U C E R B D H J K M
P	P Q T V W X Z F L Y I N G S A U C E R B D H J K M O
Q	Q T V W X Z F L Y I N G S A U C E R B D H J K M O P
R	R B D H J K M O P Q T V W X Z F L Y I N G S A U C E
S	S A U C E R B D H J K M O P Q T V W X Z F L Y I N G
T	T V W X Z F L Y I N G S A U C E R B D H J K M O P Q
U	U C E R B D H J K M O P Q T V W X Z F L Y I N G S A
V	V W X Z F L Y I N G S A U C E R B D H J K M O P Q T
W	W X Z F L Y I N G S A U C E R B D H J K M O P Q T V
X	X Z F L Y I N G S A U C E R B D H J K M O P Q T V W
Y	Y I N G S A U C E R B D H J K M O P Q T V W X Z F L
Z	Z F L Y I N G S A U C E R B D H J K M O P Q T V W X

Again, the column property holds.

Again it should be obvious how to factor the Q2 cipher. Since each row in the Vigenère tableau is replaced by a shifted base key, we see that the Q2 is equivalent to a Vigenère cipher followed by a monoalphabetic substitution [8] [9]:

$$C \;=\; Q_2\,(k_{\text{alpha}},\, k_{\text{shift}},\, P) \;=\; S\,(k_{\text{alpha}},\, (V\,(k_{\text{shift}}{}',\, P))$$

Here the alphabet key is the base key, but the shift key $k_{\text{shift}}{}'$ here is not the same as the keyword k_{shift} that was input into the Q2 cipher, but rather the string of characters given by

$$k_{\text{shift}}{}' \;=\; S^{-1}\,(k_{\text{alpha}},\, k_{\text{shift}})$$

The factorization of the cipher means that each alphabetic permutation in its tableau is has the form $k \circ R_n$, and the so the set

$$Q_2[k] = \{k \circ R_n\}$$

is a *left coset* of the Vigenère set $\mathcal{V}$. Again, this set does not form a group and is not closed under composition of permutations. We pause here to point out that to rotate a permutation, we compose with the rotation on the right; this is worth remembering.

Quagmire 3 cipher

The *quagmire 3* (Q3) cipher shares the features of both the Q1 and Q2 ciphers. The plaintext alphabet across the top of the table is mixed as the base key, and the rows in the table's body are shifted versions of that base key [1] [2]. For our example:

shift key letters	plaintext letters
	F L Y I N G S A U C E R B D H J K M O P Q T V W X Z
A	A U C E R B D H J K M O P Q T V W X Z F L Y I N G S
B	B D H J K M O P Q T V W X Z F L Y I N G S A U C E R
C	C E R B D H J K M O P Q T V W X Z F L Y I N G S A U
D	D H J K M O P Q T V W X Z F L Y I N G S A U C E R B
E	E R B D H J K M O P Q T V W X Z F L Y I N G S A U C
F	F L Y I N G S A U C E R B D H J K M O P Q T V W X Z
G	G S A U C E R B D H J K M O P Q T V W X Z F L Y I N
H	H J K M O P Q T V W X Z F L Y I N G S A U C E R B D
I	I N G S A U C E R B D H J K M O P Q T V W X Z F L Y
J	J K M O P Q T V W X Z F L Y I N G S A U C E R B D H
K	K M O P Q T V W X Z F L Y I N G S A U C E R B D H J
L	L Y I N G S A U C E R B D H J K M O P Q T V W X Z F
M	M O P Q T V W X Z F L Y I N G S A U C E R B D H J K
N	N G S A U C E R B D H J K M O P Q T V W X Z F L Y I
O	O P Q T V W X Z F L Y I N G S A U C E R B D H J K M
P	P Q T V W X Z F L Y I N G S A U C E R B D H J K M O
Q	Q T V W X Z F L Y I N G S A U C E R B D H J K M O P
R	R B D H J K M O P Q T V W X Z F L Y I N G S A U C E
S	S A U C E R B D H J K M O P Q T V W X Z F L Y I N G
T	T V W X Z F L Y I N G S A U C E R B D H J K M O P Q
U	U C E R B D H J K M O P Q T V W X Z F L Y I N G S A
V	V W X Z F L Y I N G S A U C E R B D H J K M O P Q T
W	W X Z F L Y I N G S A U C E R B D H J K M O P Q T V
X	X Z F L Y I N G S A U C E R B D H J K M O P Q T V W
Y	Y I N G S A U C E R B D H J K M O P Q T V W X Z F L
Z	Z F L Y I N G S A U C E R B D H J K M O P Q T V W X

After we straighten the plaintext alphabet by moving the columns, we have this tableau:

shift key letters	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	H	P	K	Q	M	A	B	T	E	V	W	U	X	R	Z	F	L	O	D	Y	J	I	N	G	C	S
B	P	X	T	Z	V	B	M	F	J	L	Y	D	I	K	N	G	S	W	O	A	Q	U	C	E	H	R
C	K	T	O	V	P	C	H	W	B	X	Z	E	F	D	L	Y	I	Q	J	N	M	G	S	A	R	U
D	Q	Z	V	F	W	D	O	L	K	Y	I	H	N	M	G	S	A	X	P	U	T	C	E	R	J	B
E	M	V	P	W	Q	E	J	X	D	Z	F	R	L	H	Y	I	N	T	K	G	O	S	A	U	B	C
F	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	B	M	H	O	J	G	E	P	U	Q	T	S	V	C	W	X	Z	K	R	F	D	L	Y	I	A	N
H	T	F	W	L	X	H	P	Y	M	I	N	J	G	O	S	A	U	Z	Q	C	V	E	R	B	K	D
I	E	J	B	K	D	I	U	M	S	O	P	N	Q	A	T	V	W	H	C	X	R	Z	F	L	G	Y
J	V	L	X	Y	Z	J	Q	I	O	N	G	K	S	P	A	U	C	F	T	E	W	R	B	D	M	H
K	W	Y	Z	I	F	K	T	N	P	G	S	M	A	Q	U	C	E	L	V	R	X	B	D	H	O	J
L	U	D	E	H	R	L	S	J	N	K	M	Y	O	G	P	Q	T	B	A	V	C	W	X	Z	I	F
M	X	I	F	N	L	M	V	G	Q	S	A	O	U	T	C	E	R	Y	W	B	Z	D	H	J	P	K
N	R	K	D	M	H	N	C	O	A	P	Q	G	T	U	V	W	X	J	E	Z	B	F	L	Y	S	I
O	Z	N	L	G	Y	O	W	S	T	A	U	P	C	V	E	R	B	I	X	D	F	H	J	K	Q	M
P	F	G	Y	S	I	P	X	A	V	U	C	Q	E	W	R	B	D	N	Z	H	L	J	K	M	T	O
Q	L	S	I	A	N	Q	Z	U	W	C	E	T	R	X	B	D	H	G	F	J	Y	K	M	O	V	P
R	O	W	Q	X	T	R	K	Z	H	F	L	B	Y	J	I	N	G	V	M	S	P	A	U	C	D	E
S	D	O	J	P	K	S	R	Q	C	T	V	A	W	E	X	Z	F	M	B	L	H	Y	I	N	U	G
T	Y	A	N	U	G	T	F	C	X	E	R	V	B	Z	D	H	J	S	L	K	I	M	O	P	W	Q
U	J	Q	M	T	O	U	D	V	R	W	X	C	Z	B	F	L	Y	P	H	I	K	N	G	S	E	A
V	I	U	G	C	S	V	L	E	Z	R	B	W	D	F	H	J	K	A	Y	M	N	O	P	Q	X	T
W	N	C	S	E	A	W	Y	R	F	B	D	X	H	L	J	K	M	U	I	O	G	P	Q	T	Z	V
X	G	E	A	R	U	X	I	B	L	D	H	Z	J	Y	K	M	O	C	N	P	S	Q	T	V	F	W
Y	C	H	R	J	B	Y	A	K	G	M	O	I	P	S	Q	T	V	D	U	W	E	X	Z	F	N	L
Z	S	R	U	B	C	Z	N	D	Y	H	J	F	K	I	M	O	P	E	G	Q	A	T	V	W	L	X

Constructed in this manner, the tableau is symmetric about the main diagonal. And again we have the column property: each letter appears exactly once in each column.

As we can see from its construction, the quagmire 3 cipher can be factored into a Vigenère cipher between two monoalphabetic substitutions [9]:

$$Q_3\ (k_{\text{alpha}}, k_{\text{shift}}, t)\ =\ S\ (k_{\text{alpha}}, V\ (k_{\text{shift}}', S^{-1}\ (k_{\text{alpha}}, t)))$$

As with the Q2, the shift key is modified as

$$k_{\text{shift}}'\ =\ S^{-1}\ (k_{\text{alpha}}, k_{\text{shift}})$$

From this factorization we can see that each of the permutations of the Q3 has the form $k \circ R_n \circ k^{-1}$, where k is our base key.

The set of permutations in the quagmire 3 tableau we denote as

$$\mathcal{Q}_3\,[k] \;=\; \{k \circ R_n \circ k^{-1}\}$$

The base key k is part of its name, since each base key has its own set of twenty-six permutations. This set is, in fact, a group under the composition of permutations. We have closure:

$$\begin{aligned} q_m \circ q_n \;&=\; (k \circ R_m \circ k^{-1}) \circ (k \circ R_n \circ k^{-1}) \\ &=\; k \circ R_m \circ (k^{-1} \circ k^{1}) \circ R_n \circ k^{-1} \\ &=\; k \circ R_m \circ e \circ R_n \circ k^{-1} \\ &=\; k \circ (R_m \circ R_n) \circ k^{-1} \\ &=\; k \circ R_{m+n} \circ k^{-1} \end{aligned}$$

The addition in the subscript is done modulo 26, and therefore we obtain another element of $\mathcal{Q}_3\,[k]$. The identity element is present:

$$k \circ R_0 \circ k^{-1} \;=\; k \circ e \circ k^{-1} \;=\; k \circ k^{-1} \;=\; e$$

And we have inverses:

$$q_n^{-1} \;=\; k \circ R_{-n} \circ k^{-1}$$

$$\begin{aligned} q_n \circ q_n^{-1} \;&=\; (k \circ R_{-n} \circ k^{-1}) \circ (k \circ R_n \circ k^{-1}) \\ &=\; k \circ R_{-n} \circ (k^{-1} \circ k) \circ R_n \circ k^{-1} \\ &=\; k \circ R_{-n} \circ e \circ R_n \circ k^{-1} \\ &=\; k \circ (R_{-n} \circ R_n) \circ k^{-1} \\ &=\; k \circ R_0 \circ k^{-1} \\ &=\; e \end{aligned}$$

The transformation

$$\varphi\,(R_n) \;=\; k \circ R_n \circ k^{-1}$$

is actually an isomorphism from the Vigenère set to $\mathcal{Q}_3\,[k]$. We see that this is so because it preserves the group structure:

$$\begin{aligned} \varphi\,(R_m \circ R_n) \;&=\; k \circ (R_m \circ R_n) \circ k^{-1} \\ &=\; k \circ R_m \circ e \circ R_n \circ k^{-1} \\ &=\; k \circ R_m \circ (k^{-1} \circ k) \circ R_n \circ k^{-1} \\ &=\; (k \circ R_m \circ k^{-1}) \circ (k \circ R_n \circ k^{-1}) \\ &=\; \varphi\,(R_m) \circ \varphi\,(R_n) \end{aligned}$$

So ($\mathcal{Q}_3\,[k]$, $\circ$) is isomorphic to ($\mathcal{V}$, $\circ$), which in turn, as we saw, is isomorphic to ($\mathbb{Z}_{26}$, + mod 26). We can rightly conclude that ($\mathcal{Q}_3\,[k]$, $\circ$) is therefore also isomorphic to ($\mathbb{Z}_{26}$, + mod 26). Important consequences of the isomorphism to $\mathcal{V}$ include the orders of the elements (1, 2, 13, and 26), and the factorization of the elements into cycles (twenty-six 1-cycles, thirteen 2-cycles, two 13-cycles, or one 26-cycle). Furthermore, we now know without checking all 26×26 possibilities that the quagmire group is commutative, since both $(\mathcal{V}, \circ)$ and $(\mathbb{Z}_{26}, + \bmod 26)$ are. And still further, we now know that the quagmire 3 group is cyclic, so that the entire tableau can be generated by taking powers of any one of the order-26 elements ("power" meaning taking successive compositions).

Quagmire 4 cipher

The *quagmire 4* (Q4) cipher extends the Q3 by using a different base key for the mixed plaintext alphabet and for the shifted key in the bulk of the table [1] [2]. As an example, we consider these two base keys:

$$k_P = \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$
$$k_C = \texttt{SPACEFLIGHTBDJKMNOQRUVWXYZ}$$

shift key	plaintext letters																									
letters	F	L	Y	I	N	G	S	A	U	C	E	R	B	D	H	J	K	M	O	P	Q	T	V	W	X	Z
A	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P
B	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T
C	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A
D	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B
E	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C
F	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E
G	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I
H	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G
I	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L
J	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D
K	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J
L	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F
M	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K
N	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M
O	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N
P	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S
Q	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O
R	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q
S	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z
T	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H
U	U	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R
V	V	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U
W	W	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V
X	X	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W
Y	Y	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X
Z	Z	S	P	A	C	E	F	L	I	G	H	T	B	D	J	K	M	N	O	Q	R	U	V	W	X	Y

After we straighten out the plaintext alphabet, we have a tableau of alphabetic permutations:

shift key	plaintext letters																									
letters	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	H	K	B	M	D	A	I	N	F	O	Q	C	R	L	U	V	W	J	G	X	T	Y	Z	S	E	P
B	Q	X	U	Y	V	B	N	Z	K	S	P	D	A	M	C	E	F	W	O	L	R	I	G	H	J	T
C	T	M	D	N	J	C	G	O	L	Q	R	E	U	I	V	W	X	K	H	Y	B	Z	S	P	F	A
D	R	Y	V	Z	W	D	O	S	M	P	A	J	C	N	E	F	L	X	Q	I	U	G	H	T	K	B
E	B	N	J	O	K	E	H	Q	I	R	U	F	V	G	W	X	Y	M	T	Z	D	S	P	A	L	C
F	D	O	K	Q	M	F	T	R	G	U	V	L	W	H	X	Y	Z	N	B	S	J	P	A	C	I	E
G	M	U	O	V	Q	G	J	W	B	X	Y	H	Z	D	S	P	A	R	K	C	N	E	F	L	T	I
H	N	V	Q	W	R	H	K	X	D	Y	Z	T	S	J	P	A	C	U	M	E	O	F	L	I	B	G
I	K	R	N	U	O	I	D	V	T	W	X	G	Y	B	Z	S	P	Q	J	A	M	C	E	F	H	L
J	U	Z	W	S	X	J	Q	P	N	A	C	K	E	O	F	L	I	Y	R	G	V	H	T	B	M	D
K	V	S	X	P	Y	K	R	A	O	C	E	M	F	Q	L	I	G	Z	U	H	W	T	B	D	N	J
L	J	Q	M	R	N	L	B	U	H	V	W	I	X	T	Y	Z	S	O	D	P	K	A	C	E	G	F
M	W	P	Y	A	Z	M	U	C	Q	E	F	N	L	R	I	G	H	S	V	T	X	B	D	J	O	K
N	X	A	Z	C	S	N	V	E	R	F	L	O	I	U	G	H	T	P	W	B	Y	D	J	K	Q	M
O	Y	C	S	E	P	O	W	F	U	L	I	Q	G	V	H	T	B	A	X	D	Z	J	K	M	R	N
P	G	J	T	K	B	P	L	M	E	N	O	A	Q	F	R	U	V	D	I	W	H	X	Y	Z	C	S
Q	Z	E	P	F	A	Q	X	L	V	I	G	R	H	W	T	B	D	C	Y	J	S	K	M	N	U	O
R	S	F	A	L	C	R	Y	I	W	G	H	U	T	X	B	D	J	E	Z	K	P	M	N	O	V	Q
S	I	D	H	J	T	S	F	K	C	M	N	P	O	E	Q	R	U	B	L	V	G	W	X	Y	A	Z
T	O	W	R	X	U	T	M	Y	J	Z	S	B	P	K	A	C	E	V	N	F	Q	L	I	G	D	H
U	P	L	C	I	E	U	Z	G	X	H	T	V	B	Y	D	J	K	F	S	M	A	N	O	Q	W	R
V	A	I	E	G	F	V	S	H	Y	T	B	W	D	Z	J	K	M	L	P	N	C	O	Q	R	X	U
W	C	G	F	H	L	W	P	T	Z	B	D	X	J	S	K	M	N	I	A	O	E	Q	R	U	Y	V
X	E	H	L	T	I	X	A	B	S	D	J	Y	K	P	M	N	O	G	C	Q	F	R	U	V	Z	W
Y	F	T	I	B	G	Y	C	D	P	J	K	Z	M	A	N	O	Q	H	E	R	L	U	V	W	S	X
Z	L	B	G	D	H	Z	E	J	A	K	M	S	N	C	O	Q	R	T	F	U	I	V	W	X	P	Y

The factorization of the Q4 is similar to the Q3, except that the keys of the two substitution ciphers are different [9]:

$$Q_4\,(k_\mathrm{P}, k_\mathrm{C}, k_\mathrm{shift}, t) \;=\; S\,(k_\mathrm{C}, V\,(k_\mathrm{shift}', S^{-1}\,(k_\mathrm{P}, t)))$$

Again the shift key is modified:

$$k_\mathrm{shift}' \;=\; S^{-1}\,(k_\mathrm{P}, k_\mathrm{shift})$$

From this factorization we can see that each of the permutations of the Q4 has the form $k_\mathrm{C} \circ R_n \circ k_\mathrm{P}^{-1}$.

We write the set of twenty-six permutations for given k_P and k_C as

$$Q_4\,[k_\mathrm{P}, k_\mathrm{C}] \;=\; \{k_\mathrm{C} \circ R_n \circ k_\mathrm{P}^{-1}\}$$

This set does not form a group. Rather, it is a coset of a quagmire 3 set. More than that, it is the right coset of one Q3 and the left coset of another Q3. The multiplier is the same for both cases:

$$h = k_C \circ k_P^{-1}$$

The $Q_4[k_P, k_C]$ is a left coset of $Q_3[k_P]$. To see this, we take an arbitrary element of the Q3 and combine on the left with h to obtain an element of the Q4:

$$\begin{aligned} h \circ (k_P \circ R_n \circ k_P^{-1}) &= (k_C \circ k_P^{-1}) \circ (k_P \circ R_n \circ k_P^{-1}) \\ &= k_C \circ (k_P^{-1} \circ k_P) \circ R_n \circ k_P^{-1} \\ &= k_C \circ e \circ R_n \circ k_P^{-1} \\ &= k_C \circ R_n \circ k_P^{-1} \end{aligned}$$

At the same time, $Q_4[k_P, k_C]$ is a right coset of $Q_3[k_C]$ with the same multiplier:

$$\begin{aligned} (k_C \circ R_n \circ k_C^{-1}) \circ h &= (k_C \circ R_n \circ k_C^{-1}) \circ (k_C \circ k_P^{-1}) \\ &= k_C \circ R_n \circ (\, k_C^{-1} \circ k_C) \circ k_P^{-1} \\ &= k_C \circ R_n \circ e \circ k_P^{-1} \\ &= k_C \circ R_n \circ k_P^{-1} \end{aligned}$$

Now, the identity element always appears in the tableau of a Q3 cipher. Therefore, h is a member of the Q4 tableau. Suppose we are in possession of a Q4 tableau; can we find h? Is is easier than that: *every* member of the Q4 table can act as an h. We can verify this by taking the inverse of an arbitrary element of the Q4 and composing it with another arbitrary element to get an element of $Q_3[k_P]$ (remember that the inversion of a composition of permutations is a composition of the inverses in reverse order):

$$\begin{aligned} q_m^{-1} \circ q_n &= (k_C \circ R_m \circ k_P^{-1})^{-1} \circ (k_C \circ R_n \circ k_P^{-1}) \\ &= ((k_P^{-1})^{-1} \circ R_m^{-1} \circ k_C^{-1}) \circ (k_C \circ R_n \circ k_P^{-1}) \\ &= k_P \circ R_{-m} \circ k_C^{-1} \circ k_C \circ R_n \circ k_P^{-1} \\ &= k_P \circ R_{-m} \circ e \circ R_n \circ k_P^{-1} \\ &= k_P \circ R_{-m} \circ R_n \circ k_P^{-1} \\ &= k_P \circ R_{n-m} \circ k_P^{-1} \end{aligned}$$

Likewise, we can compose on the right to get an element of $Q_3[k_C]$:

$$\begin{aligned} q_n \circ q_m^{-1} &= (k_C \circ R_n \circ k_P^{-1}) \circ (k_C \circ R_m \circ k_P^{-1})^{-1} \\ &= (k_C \circ R_n \circ k_P^{-1}) \circ ((k_P^{-1})^{-1} \circ R_m^{-1} \circ k_C^{-1}) \\ &= k_C \circ R_n \circ k_P^{-1} \circ k_P \circ R_{-m} \circ k_C^{-1} \\ &= k_C \circ R_n \circ e \circ R_{-m} \circ k_C^{-1} \\ &= k_C \circ R_n \circ R_{-m} \circ k_C^{-1} \\ &= k_C \circ R_{n-m} \circ k_C^{-1} \end{aligned}$$

The effect of using a different element of $Q_4[k_P, k_C]$ in place of h is merely to reorder the permutations in the $Q_3[k_P]$ or $Q_3[k_C]$. But order is irrelevant in sets, including these.

Atbash cipher

The *atbash cipher* may very well be the oldest cipher in the world. It is a monoalphabetic substitution with only one possible key. We only mention this cipher because its permutation is a useful one. To encipher a text with atbash, we replace each letter according to this guide:

```
ABCDEFGHIJKLM
↕↕↕↕↕↕↕↕↕↕↕↕↕
ZYXWVUTSRQPON
```

The alphabetic permutation for this cipher, which we call *z* for no good reason whatsoever, is

$$z = \mathtt{ZYXWVUTSRQPONMLKJIHGFEDCBA}$$

Encryption and decryption are the same process; the cipher is involutory. In other words,

$$z \circ z = e$$

If we want to think about this cipher numerically by assigning A = 0, B = 1, ..., then the action of the cipher is to take letter number n to $-(n + 1)$ modulo 26.

Notice, too, that *z* is the same as the affine permutation $A_{25,25}$, which we may also write as $A_{-1,-1}$.

Beaufort cipher

The *Beaufort cipher* [1] [2] is a periodic polyalphabetic substitution cipher whose tableau is completely known, like the Vigenère. Here is its tableau:

key	plaintext letters	label of
letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ	permutation
A	AZYXWVUTSRQPONMLKJIHGFEDCB	b_{25}
B	BAZYXWVUTSRQPONMLKJIHGFEDC	b_{24}
C	CBAZYXWVUTSRQPONMLKJIHGFED	b_{23}
D	DCBAZYXWVUTSRQPONMLKJIHGFE	b_{22}
E	EDCBAZYXWVUTSRQPONMLKJIHGF	b_{21}
F	FEDCBAZYXWVUTSRQPONMLKJIHG	b_{20}
G	GFEDCBAZYXWVUTSRQPONMLKJIH	b_{19}
H	HGFEDCBAZYXWVUTSRQPONMLKJI	b_{18}
I	IHGFEDCBAZYXWVUTSRQPONMLKJ	b_{17}
J	JIHGFEDCBAZYXWVUTSRQPONMLK	b_{16}
K	KJIHGFEDCBAZYXWVUTSRQPONML	b_{15}
L	LKJIHGFEDCBAZYXWVUTSRQPONM	b_{14}
M	MLKJIHGFEDCBAZYXWVUTSRQPON	b_{13}
N	NMLKJIHGFEDCBAZYXWVUTSRQPO	b_{12}
O	ONMLKJIHGFEDCBAZYXWVUTSRQP	b_{11}

P	PONMLKJIHGFEDCBAZYXWVUTSRQ	b_{10}
Q	QPONMLKJIHGFEDCBAZYXWVUTSR	b_9
R	RQPONMLKJIHGFEDCBAZYXWVUTS	b_8
S	SRQPONMLKJIHGFEDCBAZYXWVUT	b_7
T	TSRQPONMLKJIHGFEDCBAZYXWVU	b_6
U	UTSRQPONMLKJIHGFEDCBAZYXWV	b_5
V	VUTSRQPONMLKJIHGFEDCBAZYXW	b_4
W	WVUTSRQPONMLKJIHGFEDCBAZYX	b_3
X	XWVUTSRQPONMLKJIHGFEDCBAZY	b_2
Y	YXWVUTSRQPONMLKJIHGFEDCBAZ	b_1
Z	ZYXWVUTSRQPONMLKJIHGFEDCBA	$b_0 = z$

If we prefer to work with numbers rather than a tableau, and assign A = 0, B = 1, ..., Z = 25, then the action of the cipher is

$$\begin{aligned} c_i &= (k_{i \bmod L} - p_i) \bmod 26 \\ p_i &= (k_{i \bmod L} - c_i) \bmod 26 \end{aligned}$$

where L is the length of the key and p_i and c_i are the numbers of the i^{th} plaintext and ciphertext letters.

We return now to the tableau. The first thing to notice is that the last permutation is z, the atbash key. Like it, all of the permutations in the table are self-reciprocal (involutory), and hence so is the entire cipher. Each of the permutations is also a rotation of z. With the labels that we have assigned them,

$$b_n = z \circ R_n$$

Each of the b_n is also an affine permutation:

$$b_n = A_{-1,\,-n-1}$$

or

$$b_{-n} = A_{-1,\,n-1}$$

Had we numbered them from the top down, these last two equations would have been a bit cleaner.

Since every member of the Beaufort set $\mathcal{B}$ of permutations is a rotation of the same base key z, we see that the Beaufort cipher is a quagmire 2:

$$\mathcal{B} = \{b_n\} = \{z \circ R_n\} = \mathcal{Q}_2[z]$$

Without proving it, we state here that to reverse a permutation, we compose with z on the right. Now, a rightward rotation by n steps is the same as a leftward rotation by $-n$ steps (modulo 26). To make a leftward rotation, we can reverse, take a rightward rotation, then reverse again:

$$R_n = z \circ R_{-n} \circ z$$

Compose with z on the left on both sides of the equation:

$$\begin{aligned} z \circ R_n &= z \circ (z \circ R_{-n} \circ z) \\ z \circ R_n &= (z \circ z) \circ R_{-n} \circ z \\ z \circ R_n &= e \circ R_{-n} \circ z \\ z \circ R_n &= R_{-n} \circ z \end{aligned}$$

Now it is possible to see self-reciprocity by

$$\begin{aligned} b_n \circ b_n &= (z \circ R_n) \circ (z \circ R_n) \\ &= (z \circ R_n) \circ (R_{-n} \circ z) \\ &= z \circ (R_n \circ R_{-n}) \circ z \\ &= z \circ e \circ z = z \circ z = e \end{aligned}$$

Furthermore, since we now know that each Beaufort permutation can be written as a rotation composed with z on the right, we see that $\mathcal{B}$ is also a quagmire 1 set (note that $\{R_{-n}\}$ is the same as $\{R_n\}$; they contain the same twenty-six permutations):

$$\mathcal{B} = \{b_n\} = \{z \circ R_n\} = \{R_{-n} \circ z\} = \{R_n \circ z\} = Q_1[z]$$

Let us digress for a bit and look more at the permutations b_n and their products. Since each b_n has the form of the composition of z with a rotation, it should be no surprise that the product of a b with an R is another b:

$$b_m \circ R_n = (z \circ R_m) \circ R_n \qquad = z \circ R_{m+n} = b_{m+n}$$

$$R_n \circ b_m = R_n \circ (z \circ R_m) = R_n \circ (R_{-m} \circ z) = R_{n-m} \circ z = z \circ R_{m-n} = b_{m-n}$$

As usual, all of the arithmetic in the subscripts is performed modulo 26. The composition of the Beaufort permutations is a rotation:

$$\begin{aligned} b_m \circ b_n &= (z \circ R_m) \circ (z \circ R_n) \\ &= (R_{-m} \circ z) \circ (z \circ R_n) \\ &= R_{-m} \circ (z \circ z) \circ R_n \\ &= R_{-m} \circ e \circ R_n \\ &= R_{-m} \circ R_n = R_{n-m} \end{aligned}$$

There is a sort of antisymmetry in that last equation: if we reverse the order of the factors, the result is a rotation in the opposite direction.

Since each b_n is one of the affine permutations, the composition of a Beaufort with an affine permutation will give another affine permutation. Recall that

$$A_{c,d} \circ A_{a,b} = A_{a \cdot c,\, b \cdot c+d}$$

and

$$b_n = A_{-1,\, -n-1}$$

So

$$b_m \circ A_{n,p} \;=\; A_{-1,\,-m-1} \circ A_{n,p} \;=\; A_{-n,\,-p-m-1}$$

and

$$A_{n,p} \circ b_m \;=\; A_{n,p} \circ A_{-1,\,-m-1} \;=\; A_{-n,\,p-n-m\cdot n}$$

If we compose with $b_m^{-1} = b_m$ on the left of both sides of the first of these, we have

$$A_{n,p} \;=\; b_m \circ A_{-n,\,-p-m-1}$$

Doing so on the right of both sides of the second equation gives

$$A_{n,p} \;=\; A_{-n,\,p-n-m\cdot n} \circ b_m$$

Equating the two gives

$$b_m \circ A_{-n,\,-p-m-1} \;=\; A_{-n,\,p-n-m\cdot n} \circ b_m$$

Changing variables $n \to -n$ (if n is invertible, then so is $-n$) and $p \to -p-m-1$ allows us to write

$$b_m \circ A_{n,p} \;=\; A_{n,\,m\cdot n-m+n-p-1} \circ b_m$$

A different change of variables in the subscripts allows us to also write

$$A_{n,p} \circ b_m \;=\; b_m \circ A_{n,\,m\cdot n-m+n-p-1}$$

The subscripts may have become somewhat complicated, but the result is relatively simple, and will be useful later.

Beaufort, Vigenère, and the dihedral group

We saw earlier that the set of permutations in the Beaufort cipher do not form a closed set under the composition operation. Explicitly, we saw this because the composition of two of them results in a rotation, which is not in the set:

$$b_m \circ b_n \;=\; R_{n-m}$$

Suppose now that we want to make a group out of $\{b_n\}$. We need to add the rotations $\{R_n\}$, but nothing else, because we also saw earlier that the composition of a b with an R is another b:

$$\begin{gathered} b_m \circ R_n \;=\; b_{m+n} \\ R_m \circ b_n \;=\; b_{m-n} \end{gathered}$$

and we already know that composing two rotations is another rotation:

$$R_m \circ R_n \;=\; R_{m+n}$$

The union of the Vigenère and Beaufort sets, therefore, is closed. It is also a group, since it contains the identity element $e = R_0$, and every element has an inverse:

$$\begin{aligned} R_n^{-1} \;&=\; R_{-n} \\ b_n^{-1} \;&=\; b_n \end{aligned}$$

This group is isomorphic to something called the *dihedral group* on twenty-six objects:

$$(\{R_n\} \cup \{b_n\}, \circ) \;\cong\; D_{52}$$

Notice that it is called D_{52}, because it contains fifty-two elements. But be aware that some call it D_{26}, because its elements operate on twenty-six objects (for us, the letters of the alphabet). So when you meet a stranger on the street and start discussing dihedral groups, make sure that you agree on your naming convention. You don’t want any unnecessary embarrassment; believe me, I know. Notice also that we did not specify the binary operator for D_{52}. For now, let us just think of it abstractly.

There are a couple (or more) ways of thinking about the dihedral group. One is as the span of two elements, often called a and x. They have these three properties:

$$\begin{aligned} a^{26} \;&=\; e \\ x^2 \;&=\; e \\ xax^{-1} \;&=\; a^{-1} \end{aligned}$$

Mathematicians write the span in angled brackets (“⟨⟩”), much like we use curly braces for sets. The span is the set of all possible multiples and powers of the two generating elements. In our case, we would write

$$D_{52} \;=\; \langle\, a, x \;|\; a^{26} = x^2 = e, xax^{-1} = a^{-1} \,\rangle$$

We know from $x^2 = e$ that $x^{-1} = x$, so we can drop the “$^{-1}$” from x whenever we wish. The most natural way to fit our set of fifty-two permutations of the alphabet with the description above by assigning $a = R_1$ and $x = b_0 = z$. We already know that

$$R_1^{26} \;=\; R_{26} \;=\; R_0 \;=\; e$$

and

$$b_0 \circ b_0 \;=\; \mathrm{e}$$

But what about the third property? Let’s see:

$$\begin{aligned} b_0 \circ R_1 \circ b_0 \;&=\; (b_0 \circ R_1) \circ b_0 \\ &=\; b_{1+0} \circ b_0 \;=\; b_1 \circ b_0 \\ &=\; R_{-1} \;=\; R_{25} \;=\; R_1^{-1} \end{aligned}$$

We have a match. In fact, for any b and R,

$$b_m \circ R_n \circ b_m \;=\; b_{m+n} \circ b_m \;=\; R_{n-(m+n)} \;=\; R_{-m} \;=\; R_m^{-1}$$

Another popular way to represent the dihedral group is this way:

$$D_{52} \;=\; \langle\, x, y \;|\; x^2 = y^2 = (xy)^{26} = e \,\rangle$$

The mathematician reading this is screaming “Hey! That’s a *Coxeter group*!” and s/he is correct: dihedral groups are a type of Coxeter groups. Notice that in this way of doing things, we have the span of two involutory (self-reciprocal) elements, so they must be from the set $\{b_n\}$. But this is okay, since the composition of two of them is one of the $\{R_n\}$. A natural choice for x and y is

$$x \;=\; b_0$$
$$y \;=\; b_1$$

Then

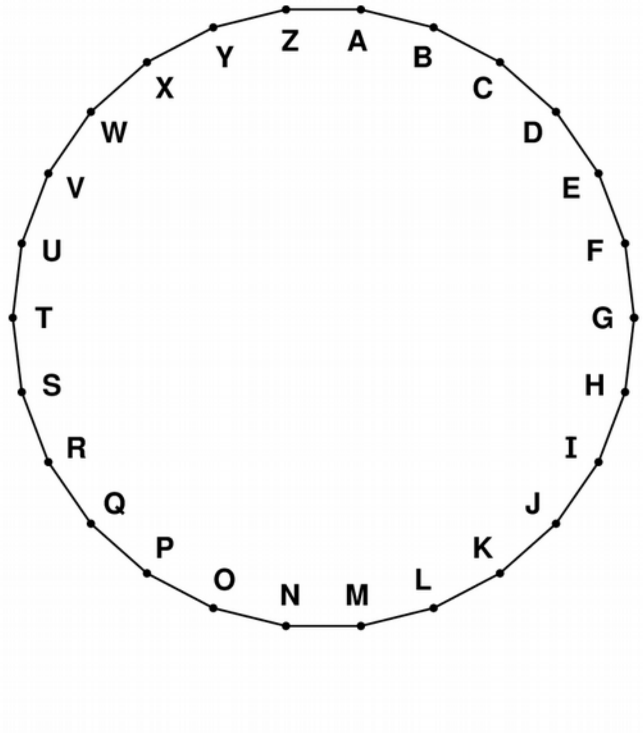
$$xy \;=\; b_0 \circ b_1 \;=\; R_1$$

so, of course,

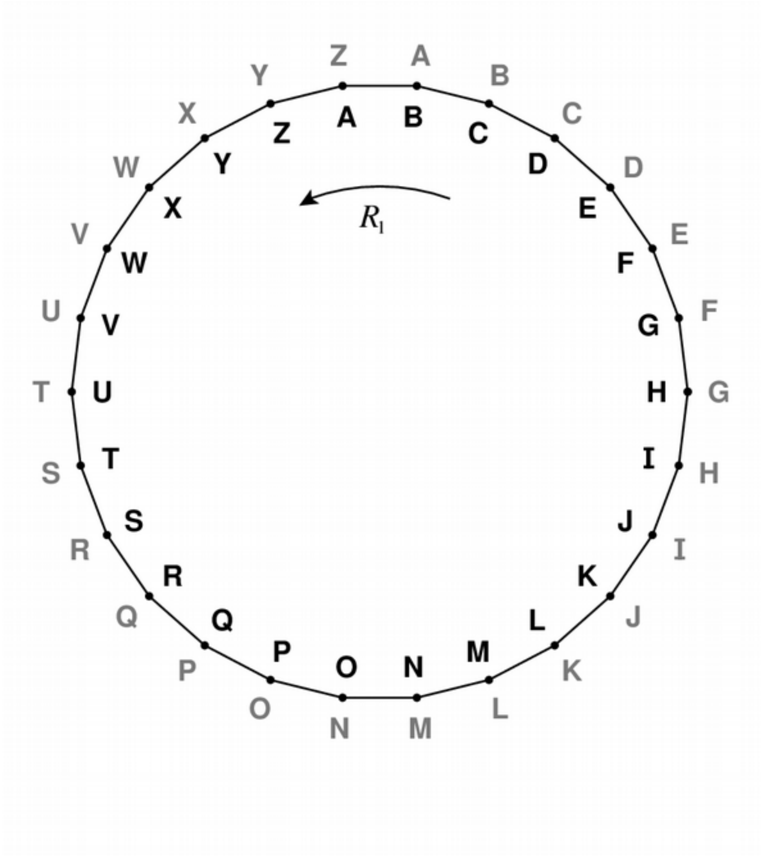
$$(xy)^{26} \;=\; R_1^{26} \;=\; e$$

What we have done here is show that any element of D_{52} can be built as a product of reflections, and we only need to use two of them to generate the entire set. If the sum of the exponents of the two generators is even, then the result is a rotation; if it is odd, then a reflection.

Another way to think of the dihedral group on n objects is as the symmetries of a rigid regular n-sided polygon (“regular” means that all sides have the same length and all angles are the same). In other words, what can we do to such a shape so that it still looks the same? For us, the shape is this regular 26-gon:

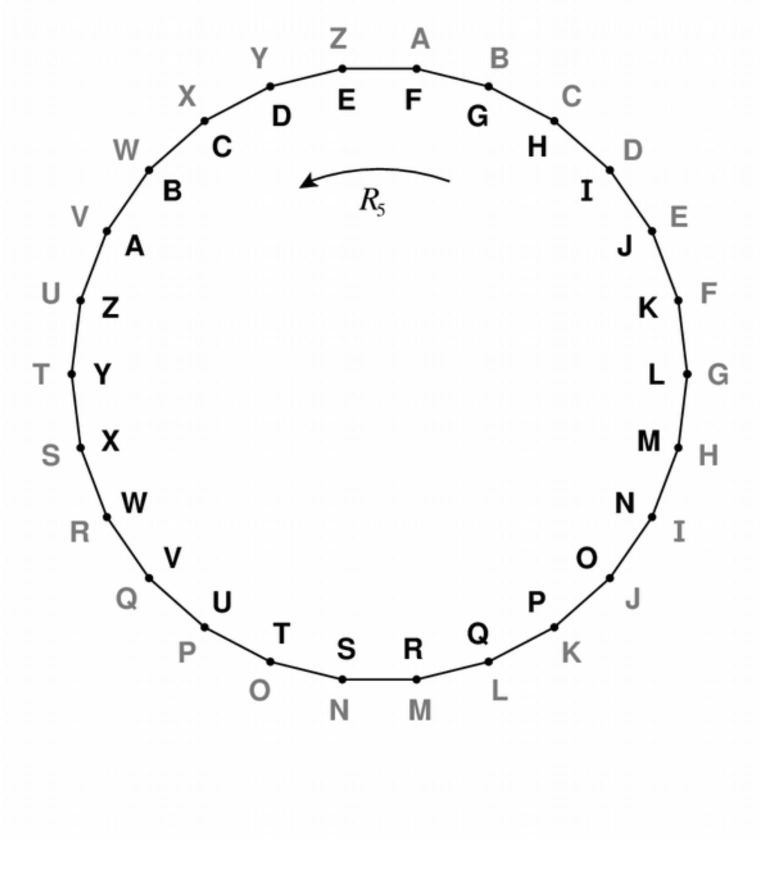


There are two types of operations that we can perform on it so that its vertices hit the same points in the plane: rotations and reflections. The effect of the rotation R_1, for example, can be seen below:



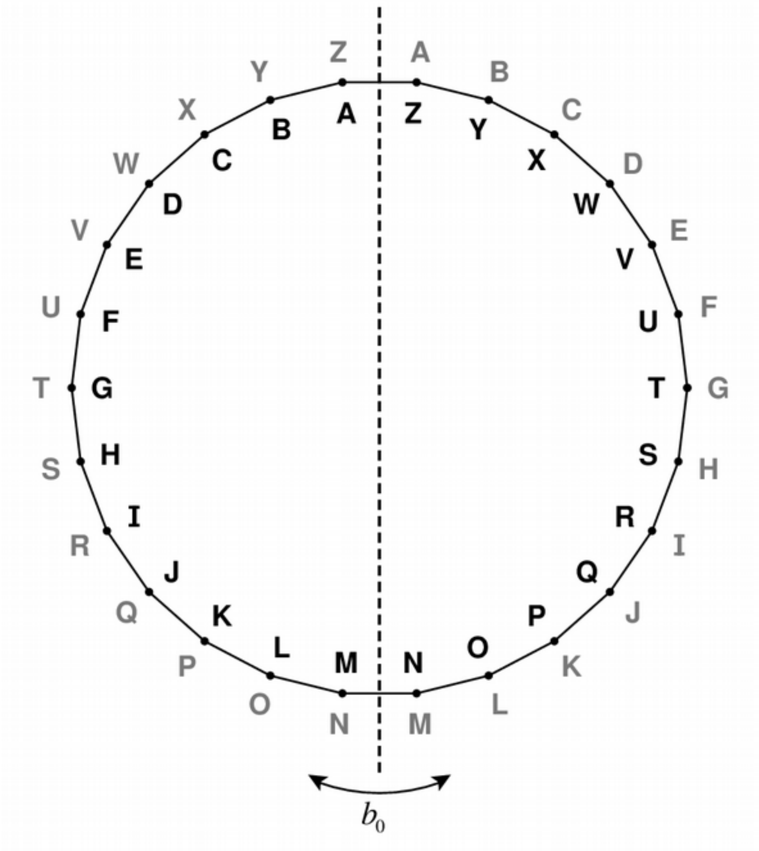
Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
R_1

Where A used to be, B now appears; where B was, now C is; etc. The rotation is counterclockwise by one step. Any rotations R_n will likewise be by n steps. Here see, for example, R_5:

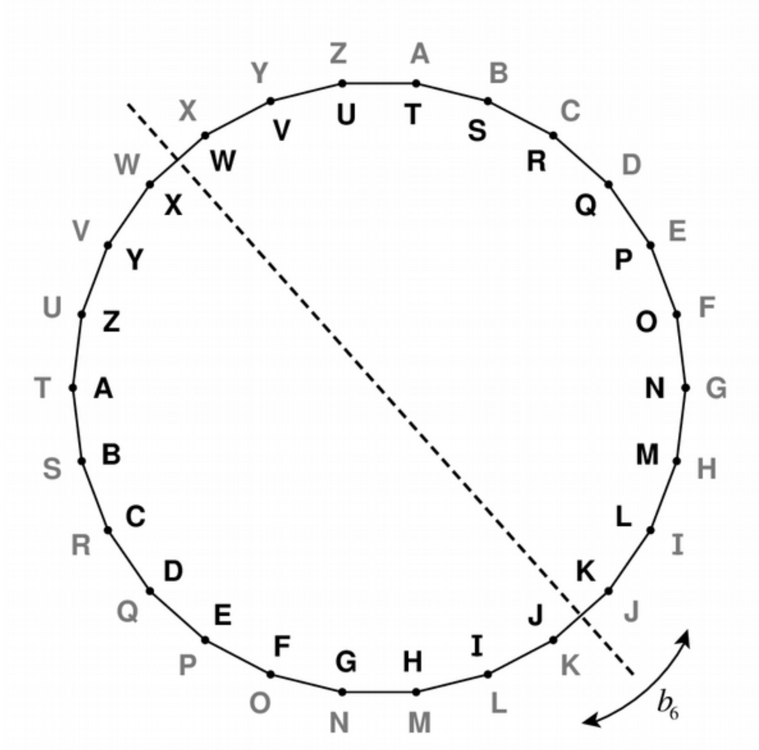


Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
R_5

The reflections (flips) are done with the $\{b_n\}$. We chose b_0 to be our generating reflection; its action can be seen in this diagram:



Each of the $\{b_n\}$ is a reflection across a different axis. For example,



We now have the ability to find compositions of rotations and reflections by playing with the 26-gon. We can show that the abstract properties of the dihedral group are held in the concrete world of geometry. We could, but we are too tired to draw any more diagrams.

We end this section by noting that if we transform each element of $\{R_n\} \cup \{b_n\}$ with some permutation k (by sandwiching each between k and k^{-1}), we see that

$$D_{52} \;\cong\; (\mathcal{V} \cup \mathcal{B}, \circ) \;=\; (\{R_n\} \cup \{b_n\}, \circ) \;\cong\; (Q_3\,[k] \cup Q_4\,[k, k \circ z], \circ)$$

Periodic affine ciphers

Recall that the permutation for the multiplication cipher with multiplier 1 is $M_1 = e$, and that affine permutations are

$$A_{m,n} \;=\; R_n \circ M_m$$

So each of the rotations can be written as

$$R_n \;=\; A_{1,n}$$

Then the Vigenère set is the set of all affine permutations with multiplier 1:

$$\mathcal{V} \;=\; \{R_n\} \;=\; \{A_{1,n}\}$$

In the previous section, we also saw that each Beaufort permutation is one of the affine permutations with multiplier 25 = −1. So

$$\mathcal{B} \;=\; \{b_n\} \;=\; \{A_{25,n}\}$$

We can, of course, build a periodic polyalphabetic substitution cipher from any set of twenty-six permutations. Let us therefore consider a generic set of affine permutations that share the same multiplier $m \in \mathbb{Z}_{26}^{\,*}$:

$$\mathcal{A}\,[m] \;=\; \{A_{m,n}\}$$

The two extrema of this group of sets are $\mathcal{V} = \mathcal{A}\,[1]$ and $\mathcal{B} = \mathcal{A}\,[25]$.

An interesting property of these *periodic affine ciphers* is that they are each simultaneously quagmire 1 and quagmire 2 ciphers. That each is a quagmire 1 is obvious from the factorization of the affine permutations into the composition of a rotation and a multiplication:

$$\mathcal{A}\,[m] \;=\; \{A_{m,n}\} \;=\; \{R_n \circ M_m\} \;=\; Q_1\,[M_m^{\;-1}]$$

To see that they are also Q2 ciphers, remember that

$$M_m \circ R_n \circ M_m^{\;-1} \;=\; R_{m\cdot n}$$

Compose both sides of the equation with M_m on the right:

$$\begin{aligned} M_m \circ R_n \circ M_m^{-1} \circ M_m &= R_{m \cdot n} \circ M_m \\ M_m \circ R_n \circ e &= R_{m \cdot n} \circ M_m \\ M_m \circ R_n &= R_{m \cdot n} \circ M_m \end{aligned}$$

A change in variable $n \rightarrow m^{-1} \cdot n \pmod{26}$ takes $m \cdot n \rightarrow m^{-1} \cdot m \cdot n = n$. So

$$M_m \circ R_{n/m} = R_n \circ M_m$$

and

$$\mathcal{A}[m] = \{A_{m,n}\} = \{R_n \circ M_m\} = \{M_m \circ R_{n/m}\}$$

But the set $\{R_{n/m}\}$ is the same as the set $\{R_n\}$, since m is invertible and multiplication by m modulo 26 is an automorphism of $(\{R_n\}, \circ)$. We can now conclude that

$$\mathcal{A}[m] = \{M_m \circ R_{n/m}\} = \{M_m \circ R_n\} = \mathcal{Q}_2[M_m]$$

Porta/Bellaso cipher

The cipher known to us as the "*Porta cipher*" [1] [2] is one of Giovan Battista Bellaso's polyalphabetic ciphers that was misattributed to another cryptographer. Bellaso's tableau [10] employs the 22-letter Italian alphabet of his time:

key	plaintext letters																					
letters	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	X	Y	Z
A/B	N	O	P	Q	R	S	T	U	X	Y	Z	A	B	C	D	E	F	G	H	I	L	M
C/D	T	U	X	Y	Z	N	O	P	Q	R	S	F	G	H	I	L	M	A	B	C	D	E
E/F	Z	N	O	P	Q	R	S	T	U	X	Y	B	C	D	E	F	G	H	I	L	M	A
G/H	S	T	U	X	Y	Z	N	O	P	Q	R	G	H	I	L	M	A	B	C	D	E	F
I/L	Y	Z	N	O	P	Q	R	S	T	U	X	C	D	E	F	G	H	I	L	M	A	B
M/N	R	S	T	U	X	Y	Z	N	O	P	Q	H	I	L	M	A	B	C	D	E	F	G
O/P	X	Y	Z	N	O	P	Q	R	S	T	U	D	E	F	G	H	I	L	M	A	B	C
Q/R	Q	R	S	T	U	X	Y	Z	N	O	P	I	L	M	A	B	C	D	E	F	G	H
S/T	P	Q	R	S	T	U	X	Y	Z	N	O	L	M	A	B	C	D	E	F	G	H	I
U/X	U	X	Y	Z	N	O	P	Q	R	S	T	E	F	G	H	I	L	M	A	B	C	D
Y/Z	O	P	Q	R	S	T	U	X	Y	Z	N	M	A	B	C	D	E	F	G	H	I	L

Recently, an earlier cipher of Bellaso from 1552 was uncovered in Venice, Italy [11]. Its tableau is a superset of the above:

key	plaintext letters
letters	ABCDEFGHILMNOPQRSTUXYZ
A	NOPQRSTUXYZABCDEFGHILM
E	ZNOPQRSTUXYBCDEFGHILMA
I	YZNOPQRSTUXCDEFGHILMAB
O	XYZNOPQRSTUDEFGHILMABC
U	UXYZNOPQRSTEFGHILMABCD
B	TUXYZNOPQRSFGHILMABCDE
C	STUXYZNOPQRGHILMABCDEF
D	RSTUXYZNOPQHILMABCDEFG
F	QRSTUXYZNOPILMABCDEFGH
G	PQRSTUXYZNOLMABCDEFGHI
H	OPQRSTUXYZNMABCDEFGHIL
L	MLIHGFEDCBAZYXUTSRQPON
M	AMLIHGFEDCBYXUTSRQPONZ
N	BAMLIHGFEDCXUTSRQPONZY
P	CBAMLIHGFEDUTSRQPONZYX
Q	DCBAMLIHGFETSRQPONZYXU
R	EDCBAMLIHGFSRQPONZYXUT
S	FEDCBAMLIHGRQPONZYXUTS
T	GFEDCBAMLIHQPONZYXUTSR
X	HGFEDCBAMLIPONZYXUTSRQ
Y	IHGFEDCBAMLONZYXUTSRQP
Z	LIHGFEDCBAMNZYXUTSRQPO

The modern version, which we now call the “Porta cipher,” comes in two varieties, the choice between which depends on one’s continent. Their tableaux are combined here:

key letters		plaintext letters
ver. 1	ver. 2	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A/B	A/B	NOPQRSTUVWXYZABCDEFGHIJKLM
C/D	Y/Z	OPQRSTUVWXYZNMABCDEFGHIJKL
E/F	W/X	PQRSTUVWXYZNOLMABCDEFGHIJK
G/H	U/V	QRSTUVWXYZNOPKLMABCDEFGHIJ
I/J	S/T	RSTUVWXYZNOPQJKLMABCDEFGHI
K/L	Q/R	STUVWXYZNOPQRIJKLMABCDEFGH
M/N	O/P	TUVWXYZNOPQRSHIJKLMABCDEFG
O/P	M/N	UVWXYZNOPQRSTGHIJKLMABCDEF
Q/R	K/L	VWXYZNOPQRSTUFGHIJKLMABCDE
S/T	I/J	WXYZNOPQRSTUVEFGHIJKLMABCD
U/V	G/H	XYZNOPQRSTUVWDEFGHIJKLMABC
W/X	E/F	YZNOPQRSTUVWXCDEFGHIJKLMAB
Y/Z	C/D	ZNOPQRSTUVWXYBCDEFGHIJKLMA

It is only natural that we should modernize the original Bellaso 1552 cipher in a similar fashion. The result is a superset of the Porta. While it is arbitrary to assign key letters to each permutation, and they have no correlation to those of the the Porta cipher, we do so anyway.

key	plaintext letters
letters	ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	AMLKJIHGFEDCBYXWVUTSRQPONZ
B	BAMLKJIHGFEDCXWVUTSRQPONZY
C	CBAMLKJIHGFEDWVUTSRQPONZYX
D	DCBAMLKJIHGFEVUTSRQPONZYXW
E	EDCBAMLKJIHGFUTSRQPONZYXWV
F	FEDCBAMLKJIHGTSRQPONZYXWVU
G	GFEDCBAMLKJIHSRQPONZYXWVUT
H	HGFEDCBAMLKJIRQPONZYXWVUTS
I	IHGFEDCBAMLKJQPONZYXWVUTSR
J	JIHGFEDCBAMLKPONZYXWVUTSRQ
K	KJIHGFEDCBAMLONZYXWVUTSRQP
L	LKJIHGFEDCBAMNZYXWVUTSRQPO
M	MLKJIHGFEDCBAZYXWVUTSRQPON
N	NOPQRSTUVWXYZABCDEFGHIJKLM
O	OPQRSTUVWXYZNMABCDEFGHIJKL
P	PQRSTUVWXYZNOLMABCDEFGHIJK
Q	QRSTUVWXYZNOPKLMABCDEFGHIJ
R	RSTUVWXYZNOPQJKLMABCDEFGHI
S	STUVWXYZNOPQRIJKLMABCDEFGH
T	TUVWXYZNOPQRSHIJKLMABCDEFG
U	UVWXYZNOPQRSTGHIJKLMABCDEF
V	VWXYZNOPQRSTUFGHIJKLMABCDE
W	WXYZNOPQRSTUVEFGHIJKLMABCD
X	XYZNOPQRSTUVWDEFGHIJKLMABC
Y	YZNOPQRSTUVWXCDEFGHIJKLMAB
Z	ZNOPQRSTUVWXYBCDEFGHIJKLMA

The first thing to notice that, like all of the ciphers in this section, this modernized Porta/Bellaso cipher is self-reciprocal (involutory). Each of its permutations is its own inverse, and the processes of encipherment and decipherment are the same.

Now for something surprising: This Porta/Bellaso cipher is a quagmire 4. To demonstrate that this is true, we simply give the base keys for the Q4 that will produce the tableau above. Consider this permutation:

$$x = \texttt{AYCWEUGSIQKOMZBXDVFTHRJPLN}$$

and its reversal:

$$x \circ z \ = \ \texttt{NLPJRHTFVDXBZMOKQISGUEWCYA}$$

The set $\mathcal{P}$ of Porta/Bellaso permutations is exactly the set of Q4 permutations using these base keys:

$$\mathcal{P} \ = \ \{p_n\} \ = \{x \circ z \circ R_n \circ x^{-1}\} \ = \ Q_4\,[x, x \circ z]$$

We leave it to the reader to work them all out and verify that they are the same as those in the tableau shown above (but not necessarily in the same order).

Next consider that each permutation of the Porta/Bellaso has the form

$$k \ = \ x \circ z \circ R_n \circ x^{-1} \ = \ x \circ (z \circ R_n) \circ x^{-1} \ = \ x \circ b_n \circ x^{-1}$$

where b_n is a member of the Beaufort set. The transformation

$$\pi \ \rightarrow \ \varphi\,(\pi) \ = \ x \circ \pi \circ x^{-1}$$

for each permutation π in the group of alphabetic permutations Π, is an automorphism of Π. This is clear because

$$\begin{aligned} \varphi\,(\pi \circ \sigma) \ &= \ x \circ \pi \circ \sigma \circ x^{-1} \\ &= \ x \circ \pi \circ e \circ \sigma \circ x^{-1} \\ &= \ x \circ \pi \circ (x^{-1} \circ x) \circ \sigma \circ x^{-1} \\ &= \ (x \circ \pi \circ x^{-1}) \circ (x \circ \sigma \circ x^{-1}) \\ &= \ \varphi\,(\pi) \circ \varphi\,(\sigma) \end{aligned}$$

Under this automorphism, the Beaufort set $\mathcal{B}$ is mapped to the Porta/Bellaso set $\mathcal{P}$.

The choice of x is not unique. Any permutation of the form $x \circ A_{m,p}$ will also work:

$$\begin{aligned} (x \circ A_{m,p}) \circ b_n \circ (x \circ A_{m,p})^{-1} \ &= \ x \circ A_{m,p} \circ b_n \circ A_{m,p}{}^{-1} \circ x^{-1} \\ &= \ x \circ A_{m,p} \circ b_n \circ A_{1/m,\ -p/m} \circ x^{-1} \\ &= \ x \circ b_n \circ A_{m,\ m\cdot n+m-n-p-1} \circ A_{1/m,\ -p/m} \circ x^{-1} \\ &= \ x \circ b_n \circ A_{1,\ m\cdot n+m-n-p-p-1} \circ x^{-1} \\ &= \ x \circ b_n \circ R_{m\cdot n+m-n-p-p-1} \circ x^{-1} \\ &= \ x \circ b_{m\cdot n+m-p-p-1} \circ x^{-1} \end{aligned}$$

where we used these earlier results:

$$A_{m,p} \circ b_n \ = \ b_n \circ A_{m,\ m\cdot n+m-n-p-1}$$

$$A_{c,d} \circ A_{a,b} \ = \ A_{a\cdot c,\ b\cdot c+d}$$

It does not matter that the subscript on b has changed. This merely means that the new transformation has shuffled the Porta/Bellaso permutations around; the set is still the same.

The final question we might ask about the Porta/Bellaso cipher is about the quagmire 3 ciphers to which it is a left and right coset. As we saw earlier, to find such Q3 sets we take the inverse of any of the elements of a Q4 and compose it with each of the Q4 permutations. If we do so with the Porta/Bellaso set, we obtain the following quagmire 3. We leave off the key letters, since our choices can affect the order in which the permutations are listed, and therefore the key letters are arbitrary.

plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMAZNOPQRSTUVWXY
CDEFGHIJKLMABYZNOPQRSTUVWX
DEFGHIJKLMABCXYZNOPQRSTUVW
EFGHIJKLMABCDWXYZNOPQRSTUV
FGHIJKLMABCDEVWXYZNOPQRSTU
GHIJKLMABCDEFUVWXYZNOPQRST
HIJKLMABCDEFGTUVWXYZNOPQRS
IJKLMABCDEFGHSTUVWXYZNOPQR
JKLMABCDEFGHIRSTUVWXYZNOPQ
KLMABCDEFGHIJQRSTUVWXYZNOP
LMABCDEFGHIJKPQRSTUVWXYZNO
MABCDEFGHIJKLOPQRSTUVWXYZN
NZYXWVUTSRQPOLKJIHGFEDCBAM
ONZYXWVUTSRQPKJIHGFEDCBAML
PONZYXWVUTSRQJIHGFEDCBAMLK
QPONZYXWVUTSRIHGFEDCBAMLKJ
RQPONZYXWVUTSHGFEDCBAMLKJI
SRQPONZYXWVUTGFEDCBAMLKJIH
TSRQPONZYXWVUFEDCBAMLKJIHG
UTSRQPONZYXWVEDCBAMLKJIHGF
VUTSRQPONZYXWDCBAMLKJIHGFE
WVUTSRQPONZYXCBAMLKJIHGFED
XWVUTSRQPONZYBAMLKJIHGFEDC
YXWVUTSRQPONZAMLKJIHGFEDCB
ZYXWVUTSRQPONMLKJIHGFEDCBA

You may notice that the first is the identity permutation *e*, which must be present in every Q3, and that the last one in the list is *z*, the reversal of *e*. Looking closer, you may also notice that for every permutation in the list, its reversal also appears. What may be surprising is that the Porta/Bellaso is both the right *and* left coset of this Q3. Any of the members of $\mathcal{P}$ can serve as the multiplier *h*; we leave it to the reader to verify this.

The Fuer GOD cipher

The *Fuer GOD* cipher, also know as the *Wilhelm* cipher, was used by the Germans in World War I [12] [13]. It gets its first name from the fact that all messages sent in this cipher were addressed to the radio receiving station known by its call-letters as GOD. Everything we know about it comes from cryptanalysts opposing the Germans, so we do not have an original description of the cipher from a German source. In the literature, there are a few errors in its tableau; namely, there are duplicate letters in some rows. Errors such as these make an unambiguous decipherment impossible. From the requirement that each row should be a true permutation of the alphabet, and from the observation that letters occur in smaller permuted groups, this is our best educated guess of the correct tableau (subject to future corrections, of course):

key letters	plaintext letters A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A	E C D B A F J I G H L K O N M S P Q T R Z U X V W Y
B	B A D C F G E I H J N O K M L S R P T Q W X V Y U Z
C	C D A B G H E J F I K M P O L N T R Q S X U Z W V Y
D	B A C H D J F E G I L O N P K M S Q R U Z T Y V W X
E	A C D B H J F I G E M N L K O T R S P Q Y Z V U X W
F	W Y Z V X A B C E F D M J I G K H P L N S R O Q U T
G	V Y X U Z W C A B E D I H G F L K N M J Q O T P S R
H	U X Z W Y V A E B C F D I H G J N K M L S P O R T Q
I	X U V Z Y W A C B E D G I H J F K M O N L T R S Q P
J	
K	S Q R Y V X U Z T W B D C A E J H K I F G P M O N L
L	R T S W V Y Z U X F A C B E D J K I G H O N M P Q L
M	T R S Q Y W X Z V U E B A C D K F J I G H M L P N O
N	R Q P S Z W T V U X Y D B C A G I E J H K F O N L M
O	L O P N M Q S R T U V Z X Y W C A B H E D G J F K I
P	M O L N P S R Q X T Y W Z U V A D C B H F I K E J G
Q	
R	P O N M R T S Q W Y U X Z V C A B E D F J G K H I L
S	L M O N T Q R P S Z X U Y V W B A C D E G J H F K I
T	M O K N L Q S R P W Z T V U X Y D B A C E F J G I H
U	H F I G N M J K O L Q P S R V T Z U W X Y B E D C A
V	E D I G H F L M K P O N R Q J S U X T Z W V Y C A B
W	I E H F G L O M J K N Q P T R S X W Y U Z V B A D C
X	
Y	
Z	I F H J G N K L M P O T S R Q V Y U X Z W D B C A E

There is no information about the rows for J, Q, X, and Z, since no German messages using those key letters have been intercepted.

The Fuer GOD cipher is not a quagmire cipher. It is enough to notice that it does not have the column property to reach this conclusion. And its set of permutations do not form a group. We have presented it here as an example of a periodic polyalphabetic substitution cipher that is *not* a quagmire, and to remind us that it is always possible to construct such ciphers with arbitrary permutations.

Classification of periodic polyalphabetic substitution ciphers

We saw from the example of the Fuer GOD cipher that not all periodic polyalphabetic substitution ciphers are quagmires. However, we will now show why all quagmires are quagmire 4 ciphers. Every permutation in a Q1 cipher has the form $R_n \circ k^{-1}$. But we can compose on the right with the identity element to have $e \circ R_n \circ k^{-1}$. So

$$\mathcal{Q}_1[k] = \{R_n \circ k^{-1}\} = \{e \circ R_n \circ k^{-1}\} = \mathcal{Q}_4[k, e]$$

and thus the set of Q1 ciphers is a subset of the Q4 ciphers:

$$\{\mathcal{Q}_1\} \subset \{\mathcal{Q}_4\}$$

Likewise, every Q2 cipher is a quagmire 4:

$$\mathcal{Q}_2[k] = \{k \circ R_n\} = \{k \circ R_n \circ e\} = \mathcal{Q}_4[e, k]$$

so that

$$\{\mathcal{Q}_2\} \subset \{\mathcal{Q}_4\}$$

A quagmire 3 is simply a quagmire 4 in which both base keys are the same:

$$\mathcal{Q}_3[k] = \{k \circ R_n \circ k^{-1}\} = \mathcal{Q}_4[k, k]$$

and

$$\{\mathcal{Q}_3\} \subset \{\mathcal{Q}_4\}$$

Next we should ask if there are any overlaps among the sets $\{\mathcal{Q}_1\}$, $\{\mathcal{Q}_2\}$, and $\{\mathcal{Q}_3\}$. The Vigenère is the most special case in that it is in all three of these sets, and therefore also a member of $\{\mathcal{Q}_4\}$:

$$\mathcal{V} = \{R_n\} = \{R_n \circ e\} = \{e \circ R_n\} = \{e \circ R_n \circ e\}$$

$$\mathcal{V} \in \{\mathcal{Q}_1\} \cap \{\mathcal{Q}_2\} \cap \{\mathcal{Q}_3\} \subset \{\mathcal{Q}_4\}$$

The Vigenère, Beaufort, and other periodic affine ciphers, as we saw earlier, belong to the intersection of $\{\mathcal{Q}_1\}$ and $\{\mathcal{Q}_2\}$:

$$\mathcal{A}[m] \in \{\mathcal{Q}_1\} \cap \{\mathcal{Q}_2\}$$

Remember also that we said

$$\mathcal{A}[m] = Q_1[M_m^{-1}] = Q_2[M_m]$$

The Vigenère cipher is special, since it is a degenerate (its base keys are the identity permutation) member also of $\{Q_3\}$, and because 1 is its own inverse modulo 26. The Beaufort cipher shares the latter of these properties: as a periodic affine cipher, its multiplier (25) is also its own inverse. Furthermore, of all the periodic affine ciphers, the Beaufort is the only one that is its own reciprocal. But it is not the only one of its kind. Recall that

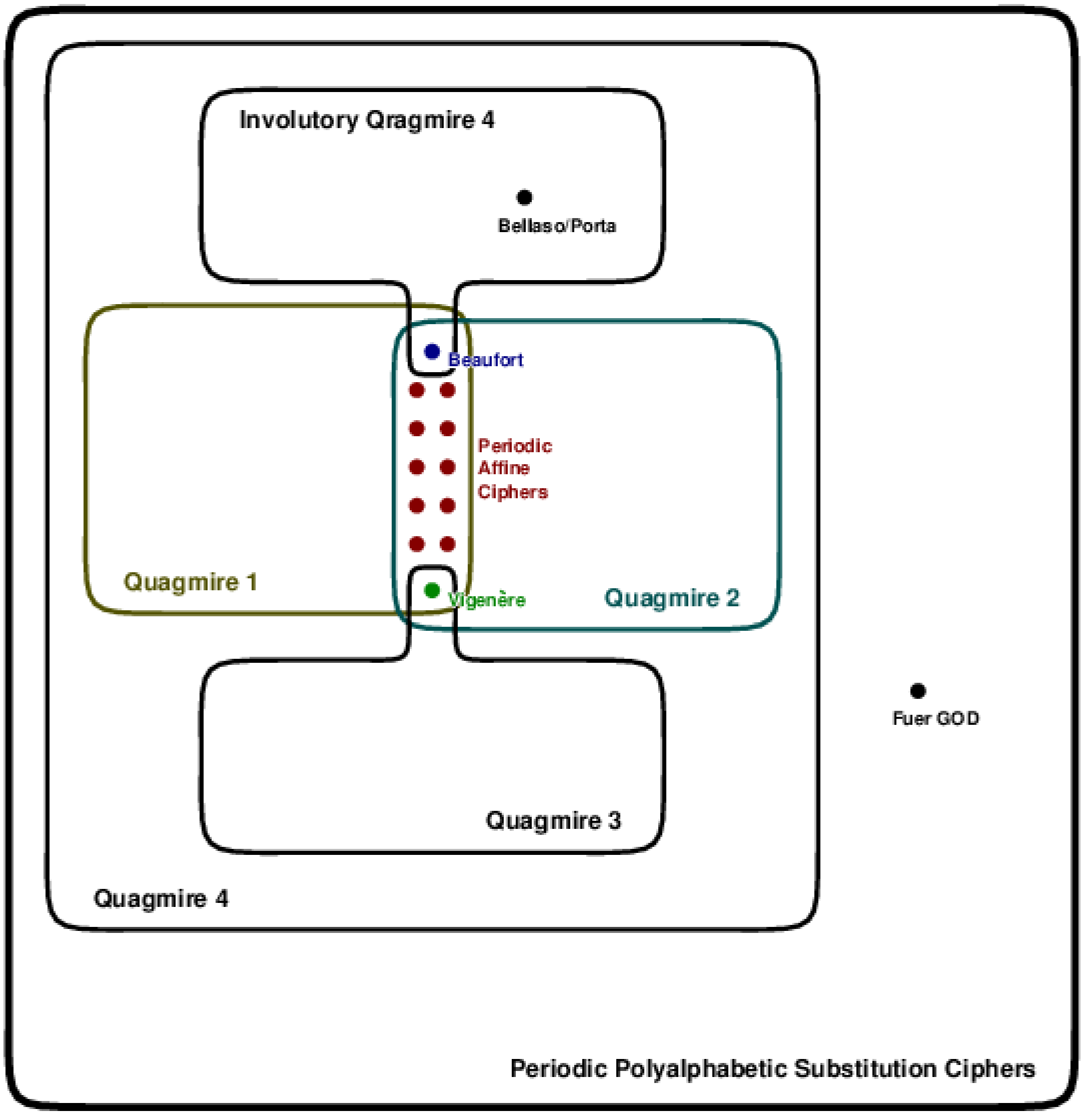
$$\mathcal{B} = \{b_n\} = \{z \circ R_n\}$$

We can insert some identity permutations and write this as

$$\mathcal{B} = \{e \circ z \circ R_n \circ e\} = \{(e \circ z) \circ R_n \circ e\} = Q_4[e, e \circ z]$$

It turns out that for any base permutation k, $Q_4[k, k \circ z]$ is an involutory quagmire 4 cipher. The base permutations for such a cipher are reversals of each other, as we see here for the Beaufort and we saw earlier for the Porta/Bellaso cipher. This class in a sense mirrors the set of quagmire 3 ciphers, whose members are all of the form $Q_4[k, k]$, where the base permutations are identical.

Here is a summary of our classification of periodic polyalphabetic substitution ciphers:


Involutory Qragmire 4
Bellaso/Porta
Beaufort
Periodic
Affine
Ciphers
Quagmire 1
Vigenère
Quagmire 2
Fuer GOD
Quagmire 3
Quagmire 4
Periodic Polyalphabetic Substitution Ciphers

Application: key amplification in crib-based attacks

When we find ourselves attacking a ciphertext, and we have been able to correctly place a crib (some snippet of known plaintext) alongside the ciphertext, then we can identify some of the letters in the permutations used to encrypt it. Henceforth, we call the set of permutations used to encrypt a text the “key table,” to distinguish it from the full tableau; the key table contains a subset of the permutations in the tableau, and may have some duplicates. But how much information do we need before we can decrypt the entire text? In the thinking of [14], information is measured in bits and calculated as the logarithm to base two of the number of possible keys. However, we want to measure the information in the keys of a cipher in terms of letters, rather than bits; therefore, we use logarithms with base twenty-six. Each of the base keys (one for quagmire 1, 2, or 3; two for quagmire 4) introduces a factor of 26! to the number of possible keys, while each shift key of length L introduces a factor of 26^L. For a Vigenère or Beaufort or Fuer GOD cipher, or any for which the tableau is fully known, the only key is the shift key, and so the information in it is

$$I \;=\; \log_{26} 26^L \;=\; L$$

letters. For a Q1, Q2, or Q3 cipher, we have one base permutation and a shift key, so the information in them is

$$I \;=\; \log_{26} (26^L \cdot 26!) \;=\; L + 18.8$$

letters. For the Q4, we have two base permutations, so

$$I \;=\; \log_{26} (26^L \cdot 26! \cdot 26!) \;=\; L + 37.6$$

letters of information. The key table contains $26{\cdot}L$ letters, so you may be wondering how to reconcile this number with such small amounts of information. The resolution of this apparent paradox is that the information contained in the table is highly redundant—each letter in a base key affects many letters in the bulk of the table.

The above are the *theoretical* lower limits to how many letters we must know in the tableau in order to completely reconstruct it. In practice, however, we find that we will need somewhat more, since the ones we have may be poorly placed and may therefore provide overlapping information. Nevertheless, we will see how a sparsely filled tableau can provide enough information to nearly fill it completely and solve the cipher.

Since we will be dealing with permutations for which we know only some of their letters, we need to be able to take compositions and find inverses for permutations with missing letters. Consider our two favorite base keys, with some holes in them:

$$k_1 \;=\; \texttt{FLYIN.S..CERB...KM..QT.WXZ}$$

$$k_2 \;=\; \texttt{SP..EF.IGHTZ.X.VUR...MKJD.}$$

Remember that this means encryption using k_1 makes these substitutions:

plaintext: `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

```
             ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:  FLYIN?S??CERB???KM??QT?WXZ
```

and using k_2 these:

```
plaintext:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
             ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:  SP??EF?IGHTZ?X?VUR???MKJDB
```

When we act with k_1 first, followed by k_2, M → B → P, for example, so the overall substitution is M → P. However, for cases in which we encounter a hole, the result is uncertain. For example, F → ? under the permutation k_1, and S → M → ? under the combined permutation. The complete list for our example is

```
plaintext:   ABCDEFGHIJKLMNOPQRSTUVWXYZ
             ↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓↓
ciphertext:  FZDGX?????ERP???T???U??KJ?
```

and we write

$$k_2 \circ k_1 = \texttt{FZDGX.....ERP...T...U..KJ.}$$

The result has more holes than either of the two factors, but there is nothing we can do about that.

Finding the inverse is done by the same method as before, simply with holes in the permutation. To find the inverse of k_1, write it under the unmixed alphabet:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
F L Y I N . S . . C E R B . . . K M . . Q T . W X Z
```

Then rearrange the columns so that letters in the lower row are in the positions they would have in the unscrambled alphabet:

```
F M J H K A I N D O Q B R E P S U L G V T W X Y C Z
. B C . E F . . I . K L M N . . Q R S T . . W X Y Z
```

Letters in the upper row above a gap are uncertain, so we replace them with gaps as well:

```
. M J . K A . . D . Q B R E . . U L G V . . X Y C Z
. B C . E F . . I . K L M N . . Q R S T . . W X Y Z
```

The upper row is now the inverse, which we know only partially:

$$k_1^{-1} = \texttt{.MJ.KA..D.QBRE..ULGV..XYCZ}$$

We are now ready to start with the Vigenère cipher and work our way to amplifying our knowledge of the keys in the quagmire 3 and 4 ciphers.

Key amplification in the Vigenère cipher

As we saw earlier, a Vigenère cipher with period *L* only has *L* letters of information in its shift key. For that reason, we only need a crib that has length *L* to fully complete its key table. This is one of only a few cases in which the theoretical information content matches our practical needs. The reader may suspect that what is needed is full knowledge of the tableau and the column property, i.e., the property that each letter appears only once in each column of the tableau. For the Vigenère we do indeed have both of these requirements. We simply need to find the subset of permutations that are used in a particular encipherment.

Here, and for the rest of this article, we will assume that we have already found the period of our cipher. The interested reader can investigate the Kasiski method [1] [15], methods using the index of coincidence [16] [17] [18], or the twist method [19].

At the risk of appearing overly pedantic, let us work an example. It is, after all, better to be clear on the fundamentals before advancing to more complicated issues. Here is a ciphertext that has been enciphered with period five:

```
SAIGR IDIVR AWTCO IRXPN CP
```

As a crib, take the first five letters of the plaintext to be `SPACE`:

```
SPACE
SAIGR IDIVR AWTCO IRXPN CP
```

Using this crib allows us to place five letters in the key table:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	S	.	.	.	.	.	.	.
k_2	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	A	.	.	.	.	.	.	.	.	.	.
k_3	I	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
k_4	.	.	G	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
k_5	.	.	.	.	R	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

We know that every permutation in the tableau of the Vigenère cipher is one of the rotations R_n of the unmixed alphabet. So we can fill in each permutation in our key table so that the known letters remain where we have placed them; they fix the rotation of each row.

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_2	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
k_3	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
k_4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
k_5	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

We now know the entire key table and can completely decrypt the text. This very simple example shows how we were able to amplify our knowledge of the key table by using what we know about the structure of the cipher. As we move on to more complicated ciphers, things will become more interesting.

Key amplification in quagmire 2

You read that correctly. We will come back to the quagmire 1 later.

Recall that the permutations in the Q2 tableau all have the form $k \circ R_n$, where k is the base key of the cipher, and the $\{R_n\}$ are the rotations of the Vigenère cipher. Permutations of this form are merely rotations of the base key. It has been known for a long time that this allows us to fill in missing letters in our key table by requiring that two letters always maintain the same distance from one another when they appear in the same row [1] [20] [21]. Another way to look at the procedure is to rotate each row of the key table until they have all aligned (have the same letter in the same column), merge them all, then rotate back to their original positions.

While this procedure is not highly technical, and in fact rather simple, we will work through an example. Here we have encrypted the opening lines of *The War of the Worlds* by H. G. Wells with period six:

```
UZMSVC CGHVZD KJNWIT ZSAVFF HOANOG HCAPCG CKVFVF IXABVM
UNETVF HGQMRQ TNVFFG MZQNTC TINWFF LAIBQQ ZHDWVF SCISTJ
SZTWIR VCRSRM SVRZVF WJTZCM TNAERQ TXJPGG TXSMVS TIJACS
TVIRZT DZZSRQ TNIRNM UBWRFM XNEWNG ZVXWED VZWBRQ ZPQHON
IZWRQL UDAEGG HOAMHM BJTTCA HPKLEM XRKVES JHRWTY ZYEPAG
TVJAES TIKPCN CAHMOG TWISHT HOIGFJ BZTTSY ZWRZZS DDQDRT
UPTWRQ ZNQPGG IJKBQN ZRVDCM DNEPRG MRQGOF XWWNRT EVLLGD
XYMUSO MRVWC
```

Our crib is the first forty-eight letters of the plaintext, which we write above its corresponding portion of the ciphertext:

```
NOONEW OULDHA VEBELI EVEDIN THELAS TYEARS OFTHEN INETEE
UZMSVC CGHVZD KJNWIT ZSAVFF HOANOG HCAPCG CKVFVF IXABVM
```

By matching plaintext and ciphertext letters, we get this information about the keys:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	.	.	.	.	Z	.	.	.	I	.	.	.	.	U	C	.	.	.	.	H	.	K	.	.	.	.
k_2	.	.	.	.	J	K	.	O	.	.	.	.	.	X	Z	.	.	.	.	.	G	S	.	.	C	.
k_3	.	N	.	.	A	.	.	.	.	.	.	H	.	.	M	.	.	.	.	V	.	.	.	.	.	.
k_4	P	.	.	V	W	.	.	F	.	.	.	N	.	S	.	.	.	.	.	B	.	.	.	.	.	.
k_5	O	.	.	.	V	.	.	Z	F	.	.	I	.	.	.	.	.	C	.	.	.	.	.	.	.	.
k_6	D	.	.	.	M	.	.	.	T	.	.	.	.	F	.	.	.	.	G	.	.	.	C	.	.	.

If we try to decrypt the entire text with this little information, we obtain

```
NOONEWOULDHAVEBELIEVEDINTHELASTYEARSOFTHENINETEEN...ENTU...
...THIS.O.L.W..BEIN...T..E..EEN.Y.N...O.EL..Y.N.E....EN.E..
RE..E....N.A.S.N..E.....R.....HI.O.N.......EN...IE...E.SE..
E.A.O.T..E...A.IO....N.E..STHE..E.E..R.T....E...D.....E..E.
.A.S.........AR.O.L.AS...N.ITH..I..O....E...H......IN..E..E
..A.SIE.T..E.T.RE...A.S....AN...L.I.....A..O.....TER
```

To amplify the keys, we take the first one as it is, but rotate the others until they are aligned:

```
....Z...I....UC....H.K....   (rotation  0)
...XZ.....GS..C.....JK.O..   (rotation 10)
.V.......N..A......H..M...   (rotation 18)
.VW..F...N.S.....B......P.   (rotation  2)
.V..ZF..I.....C........O..   (rotation  3)
T....F....G...C...D...M...   (rotation  8)
```

They can all now be merged into a single permutation:

```
TVWXZF..INGSAUC..BDHJKMOP.
```

This single permutation is then rotated in reverse into the six original positions and placed back into the key table:

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	TVWXZF..INGSAUC..BDHJKMOP.
k_2	.BDHJKMOP.TVWXZF..INGSAUC.
k_3	INGSAUC..BDHJKMOP.TVWXZF..
k_4	P.TVWXZF..INGSAUC..BDHJKMO
k_5	OP.TVWXZF..INGSAUC..BDHJKM
k_6	DHJKMOP.TVWXZF..INGSAUC..B

This is a large increase in our knowledge of the keys. With these (still incomplete) keys, we can decrypt most of the full ciphertext:

```
NOONEWOULDHAVEBELIEVEDINTHELASTYEARSOF.HENINETEENT.CENTU.Y.
.AT.HISWO.LDWASBEIN.WAT..EDKEENLYANDCLO.EL.BY.N.ELL.GENCE.G
REATE...ANMANSANDYETASMORTALA.HISO.N..ATA.MENB..IEDT.EMSEL.
E.ABO.T..EI.VARIO....NCE.NSTHEYWERE.CRUTIN..ED.ND.TUD.ED.E.
.APSALMO.TASNARROWLYASAMANWITHAMICRO.CO.EM.GHTSC.U.INI.E..E
T.ANSIENT.RE..UREST.A.SW..MANDM.L.I.L..NAD.OPOFW..ER
```

From this point, it would be easy to recognize words and fill in more letters in the plaintext and key table, until the entire plaintext is decrypted.

Key amplification in quagmire 1

Like the Q2, there is a method of key amplification that involves constant distances between letters [1] [21], using the fact that the bulk of the key table contains rotations of the unmixed alphabet. We, however, are going to try something different. Remember that every permutation in the quagmire 1 tableau have the form $R_n \circ k^{-1}$ where k is the base key. If we take the inverse of these permutations we have

$$(R_n \circ k^{-1})^{-1} = k \circ R_{-n}$$

In other words, the inverses of Q1 permutations have the form of Q2 permutations. So our strategy for key amplification will be to find the inverse of each partial key, apply the technique for the Q2, then invert back to the original key table.

An example always helps to clarify. Here is a ciphertext encrypted with period six:

```
QCTMRT ESCVVD IUNSIZ WGLVKA HYLJOC HMLPSC EKWWRA POLDRG
QFPRRA HSMKCK TFWWKC JCMJUT TQNSKA RHIDQK WXRSRA NMIMUF
NCHSIY YMEMCG NLENRA VUHNSG TFLTCK TOSPLC TOOKRR TQSASR
TLIOVZ SCYMCK TFIOYG QWJOKG ZFPSYC WLXSND YCJDCK WNMEOH
PCJOQO QTLTLC HYLKEG XUHRSE HNFLNG ZRFVNR UXESUP WVPPAC
TLSANR TQFPSH EHCKOC TBIMEZ HYIZKF XCHRZP WBENVR STMQCZ
QNHSCK WFMPLC PUFDQH WRWQSG SFPPCC JRMZOA ZBJJCZ FLDLLD
ZVTBZW JRWSS
```

Again, we will take the first forty-eight characters of the plaintext as a crib and write them above the corresponding part of the ciphertext:

```
NOONEW OULDHA VEBELI EVEDIN THELAS TYEARS OFTHEN INETEE
QCTMRT ESCVVD IUNSIZ WGLVKA HYLJOC HMLPSC EKWWRA POLDRG
```

From this we have the following knowledge of the key table:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	.	.	.	.	W	.	.	.	P	.	.	.	.	Q	E	.	.	.	.	H	.	I	.	.	.	.
k_2	.	.	.	.	U	K	.	Y	.	.	.	.	.	O	C	.	.	.	.	.	S	G	.	.	M	.
k_3	.	N	.	.	L	.	.	.	.	.	.	C	.	.	T	.	.	.	.	W	.	.	.	.	.	.
k_4	P	.	.	V	S	.	.	W	.	.	.	J	.	M	.	.	.	.	.	D	.	.	.	.	.	.
k_5	O	.	.	.	R	.	.	V	K	.	.	I	.	.	.	.	.	S	.	.	.	.	.	.	.	.
k_6	D	.	.	.	G	.	.	.	Z	.	.	.	.	A	.	.	.	.	C	.	.	.	T	.	.	.

The inverses of these six permutations are

k_1^{-1}	....O..TV......IN.....E...
k_2^{-1}	..O...V...F.Y.N...U.E...H.
k_3^{-1}	..L........E.B.....O..T...
k_4^{-1}	...T.....L..N..A..E..DH...
k_5^{-1}	........L.I...A..ER..H....
k_6^{-1}	N.SA..E............W.....I

We rotate all but one and align their columns:

....O..TV......IN.....E...	(rotation 0)
H...O...V...F.Y.N...U.E...	(rotation 24)
....O..T.....L........E.B.	(rotation 15)
H......T.....L..N..A..E..D	(rotation 22)
H............L.I...A..ER..	(rotation 21)
.........W.....IN.SA..E...	(rotation 10)

Merge them all into one:

H...O..TVW..FLYIN.SAU.ERBD

Reverse the rotations and put them back into the table of inverses:

k_1^{-1}	H...O..TVW..FLYIN.SAU.ERBD
k_2^{-1}	..O..TVW..FLYIN.SAU.ERBDH.
k_3^{-1}	.FLYIN.SAU.ERBDH...O..TVW.
k_4^{-1}	O..TVW..FLYIN.SAU.ERBDH...
k_5^{-1}	..TVW..FLYIN.SAU.ERBDH...O
k_6^{-1}	N.SAU.ERBDH...O..TVW..FLYI

Take inverses and place the results in the original key table:

	plaintext letters
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	TY.ZWM.AP..N.QE..XSHUIJ.O.
k_2	RW.XUK.YN..L.OC..VQFSGH.M.
k_3	IN.OLB.PE..C.FT..MHWJXY.D.
k_4	PU.VSI.WL..J.MA..TODQEF.K.
k_5	OT.URH.VK..I.LZ..SNCPDE.J.
k_6	DI.JGW.KZ..X.AO..HCREST.Y.

Notice that we now have the ability to decrypt the most common plaintext letters, no matter where they appear in the text.

Key amplification in quagmire 3

A method already exists for amplifying our knowledge of the permutations in the key table that exploits the fact that in the original table (in which the plaintext alphabet is deranged according to the base key) for the cipher contains rotated versions of the base key [21]. We, however, want to explore how the group structure of a Q3 cipher can be used.

Because the set of permutations $\mathcal{Q}_3[k]$ in the quagmire 3 tableau form a group isomorphic to the Vigenère group $\mathcal{V}$, we have the following features to help us amplify our knowledge of the key table and of the tableau. Keep in mind that the key table has the permutations used to encrypt a text; it is a subset of the tableau and may contain duplicate rows. The tableau contains twenty-six distinct permutations.

- Each letter of the alphabet appears exactly once in each row (permutation) in the tableau. This is the case because each row is a permuted version of the alphabet.

- The column property: each letter of the alphabet appears exactly once in each column of the tableau. This means that if we ever find two rows that share a letter in the same position, then they are the same permutation and can be merged. Note that in the key table, some rows may be the same permutation, so the column property will allow us to merge those rows, but not to remove duplicate rows.

- The set of permutations in the tableau is a group, therefore the identity element e is a member of the tableau. Combined with the column property, this means that whenever we find a permutation in which a letter of the plaintext is encrypted to itself, then that permutation is e. Furthermore, e has order 1 and is the only permutation with that order in the tableau.

- Because the tableau is a group, for any two permutations k_1 and k_2 in it, $k_1 \circ k_2$ is also in it.

- The group is commutative, so we can gain knowledge about a product by looking at both $k_1 \circ k_2$ and $k_2 \circ k_1$.

- Because the tableau is a group, for any permutation k in it, k^{-1} is also in it.

- There is exactly one member of the tableau with order 2. It can be factored into thirteen 2-cycles.

- There are exactly twelve members of the tableau with order 13. They can each be factored into two 13-cycles. Since they form a cyclic subgroup, the composition of any two of them will also be one of them.

- There are exactly twelve members of the tableau with order 26. Each is a 26-cycle. Any one of these can be used to generate the entire tableau.

Our strategy for key amplification will be to use these features and attempt to reconstruct the entire Q3 tableau. We will take compositions of rows and inverses of rows and add them to the tableau. As we work, we will merge rows as determined by the column property. The requirements that each row and each column contain exactly one of each letter may help to add missing letters or eliminate possibilities. Since knowing the structure of the permutations as products of cycles can be helpful, we will keep track of the order of each element, as we are able to determine it.

An example will be quite lengthy, but instructive. We will skip over some of the tedium. Begin with a ciphertext encrypted with a quagmire 3 with period six:

```
ZITWYE DPNSSQ MTJIPK GADSTM KZDQZP KDDFIP DRXAYM XJDHYW
ZSMYYM KPHTDL YSXATP OIHQGE YMJITM FUEHLL GXPIYM VDEWGV
VICIPJ ADSWDW VBSXYM NTCXIW YSDNDL YJQFVP YJKTYU YMQRIU
YBEZSK LIFWDL YSEZCW ZWRZTW USMICP GBZIXQ AIRHDL GHHJZX
XIRZLG ZQDNVP KZDTJW STCYIT KHAVXW UOASXU IXSIGS GVMFRP
YBQRXU YMAFIX DUNTZP YYEWJK KZEETV SICYES GYSXSU LQHLDK
ZHCIDL GSHFVP XTAHLX GOXLIW LSMFDP OOHEZM UYRQDK HBGVVQ
UVTBED OOXII
```

As usual, we present the first forty-eight letters of the plaintext as the crib, above the corresponding ciphertext:

```
NOONEW OULDHA VEBELI EVEDIN THELAS TYEARS OFTHEN INETEE
ZITWYE DPNSSQ MTJIPK GADSTM KZDQZP KDDFIP DRXAYM XJDHYW
```

Here is what we can glean about the keys:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	.	.	.	.	G	.	.	.	X	.	.	.	.	Z	D	.	.	.	.	K	.	M	.	.	.	.
k_2	.	.	.	.	T	R	.	Z	.	.	.	.	.	J	I	.	.	.	.	.	P	A	.	.	D	.
k_3	.	J	.	.	D	.	.	.	.	.	.	N	.	.	T	.	.	.	.	X	.	.	.	.	.	.
k_4	F	.	.	S	I	.	.	A	.	.	.	Q	.	W	.	.	.	.	.	H	.	.	.	.	.	.
k_5	Z	.	.	.	Y	.	.	S	T	.	.	P	.	.	.	.	.	I	.	.	.	.	.	.	.	.
k_6	Q	.	.	.	W	.	.	.	K	.	.	.	.	M	.	.	.	.	P	.	.	.	E	.	.	.

Immediately we can add the identity element to our budding tableau. It is clear that it is not one of the existing permutations, since none of them map a plaintext letter to itself. Furthermore, notice that in k_6 E → W and W → E. The presence of a 2-cycle indicates that k_6 has order 2 and can be factored into thirteen 2-cycles. This allows us to add some missing letters; for example, S → P so we can add P → S.

	plaintext letters																										
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	order
k_1	.	.	.	.	G	.	.	.	X	.	.	.	.	Z	D	.	.	.	.	K	.	M	.	.	.	.	
k_2	.	.	.	.	T	R	.	Z	.	.	.	.	.	J	I	.	.	.	.	.	P	A	.	.	D	.	
k_3	.	J	.	.	D	.	.	.	.	.	.	N	.	.	T	.	.	.	.	X	.	.	.	.	.	.	
k_4	F	.	.	S	I	.	.	A	.	.	.	Q	.	W	.	.	.	.	.	H	.	.	.	.	.	.	
k_5	Z	.	.	.	Y	.	.	S	T	.	.	P	.	.	.	.	.	I	.	.	.	.	.	.	.	.	
k_6	Q	.	.	.	W	.	.	.	K	.	I	.	N	M	.	S	A	.	P	.	.	.	E	.	.	.	2

k_7	ABCDEFGHIJKLMNOPQRSTUVWXYZ	1

Now, let us add the inverses of the permutations that we have. It is not necessary to take inverses of k_6 or k_7, as they are their own inverses.

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ	order
k_1	....G...X....ZD....K.M....	
k_2	....TR.Z.....JI.....PA..D.	
k_3	.J..D......N..T....X......	
k_4	F..SI..A...Q.W.....H......	
k_5	Z...Y..ST..P.....I........	
k_6	Q...W...K.I.NM.SA.P...E...	2
k_7	ABCDEFGHIJKLMNOPQRSTUVWXYZ	1
$k_8 = k_1^{-1}$	...O..E...T.V..........I.N	
$k_9 = k_2^{-1}$	V..Y....ON.....U.F.E.....H	
$k_{10} = k_3^{-1}$	...E.....B...L.....O...T..	
$k_{11} = k_4^{-1}$	H....A.TE.......L.D...N...	
$k_{12} = k_5^{-1}$	........R......L..HI....EA	

Remember that the Q3 group is commutative. Since there are missing letters in our permutations, we may gain different knowledge from composing two of them in one order that in the other. For k_1 and k_2 we find that

$k_1 \circ k_2$ = ...K.........X...........

but

$k_2 \circ k_1$ = ...

which is unfortunate. For k_1 and k_4 we obtain

$k_1 \circ k_4$ = ...X.....................
$k_4 \circ k_1$ = ...S...........

These must be the same permutation, so we can say that

$k_1 \circ k_4$ = ...X.........S...........

As we add compositions of permutations, we will take them in both orders and merge the results. So we proceed. Since $k_1 \circ k_1$ yields nothing new, we do not need to add it to the table.

$k_{13} = k_1 \circ k_2$	....K.........X...........	

$k_{14} = k_1 \circ k_3$	.	.	.	.	.	.	.	.	.	.	.	Z	.	.	K	.	.	.	.	.	.	.	.	.	.	.	
$k_{15} = k_1 \circ k_4$	.	.	.	.	X	.	.	.	.	.	.	.	.	.	S	.	.	.	.	.	.	.	.	.	.	.	
$k_{16} = k_1 \circ k_5$	.	.	.	.	.	.	.	.	K	.	.	.	.	.	.	.	.	X	.	.	.	.	.	.	.	.	

Let us pause for a moment to notice that k_{16} shares a K under the plaintext letter I with k_6. Therefore, they are the same permutation. We can then merge the X from k_{17} into k_6 and add an R to complete that 2-cycle.

	plaintext letters																										
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	order
k_6	Q	.	.	.	W	.	.	.	K	.	I	.	N	M	.	S	A	X	P	.	.	.	E	R	.	.	2

We continue:

$k_{17} = k_1 \circ k_6$	.	.	.	.	.	.	.	.	R	.	X	.	Z	.	.	.	.	.	.	I	.	N	G	.	.	.	

Now, k_{17} shares two letters with k_{12}, so we merge its letters into k_{12}.

k_{12}	.	.	.	.	.	.	.	.	R	.	X	.	Z	.	.	L	.	.	H	I	.	N	G	.	E	A	

This process continues for a very long time, and should be automated. We take compositions and inverses of permutations that are already in the table. Whenever possible, we merge rows. The result for this example is a complete reconstruction of the tableau (we got lucky that forty-eight was enough):

plaintext letters																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	M	H	O	J	G	E	P	U	Q	T	S	V	C	W	X	Z	K	R	F	D	L	Y	I	A	N
C	H	R	J	B	Y	A	K	G	M	O	I	P	S	Q	T	V	D	U	W	E	X	Z	F	N	L
D	O	J	P	K	S	R	Q	C	T	V	A	W	E	X	Z	F	M	B	L	H	Y	I	N	U	G
E	J	B	K	D	I	U	M	S	O	P	N	Q	A	T	V	W	H	C	X	R	Z	F	L	G	Y
F	G	Y	S	I	P	X	A	V	U	C	Q	E	W	R	B	D	N	Z	H	L	J	K	M	T	O
G	E	A	R	U	X	I	B	L	D	H	Z	J	Y	K	M	O	C	N	P	S	Q	T	V	F	W
H	P	K	Q	M	A	B	T	E	V	W	U	X	R	Z	F	L	O	D	Y	J	I	N	G	C	S
I	U	G	C	S	V	L	E	Z	R	B	W	D	F	H	J	K	A	Y	M	N	O	P	Q	X	T
J	Q	M	T	O	U	D	V	R	W	X	C	Z	B	F	L	Y	P	H	I	K	N	G	S	E	A
K	T	O	V	P	C	H	W	B	X	Z	E	F	D	L	Y	I	Q	J	N	M	G	S	A	R	U
L	S	I	A	N	Q	Z	U	W	C	E	T	R	X	B	D	H	G	F	J	Y	K	M	O	V	P
M	V	P	W	Q	E	J	X	D	Z	F	R	L	H	Y	I	N	T	K	G	O	S	A	U	B	C
N	C	S	E	A	W	Y	R	F	B	D	X	H	L	J	K	M	U	I	O	G	P	Q	T	Z	V
O	W	Q	X	T	R	K	Z	H	F	L	B	Y	J	I	N	G	V	M	S	P	A	U	C	D	E

PXTZVBMFJLYDIKNGSWOAQUCEHR
QZVFWDOLKYIHNMGSAXPUTCERJB
RKDMHNCOAPQGTUVWXJEZBFLYSI
SRUBCZNDYHJFKIMOPEGQATVWLX
TFWLXHPYMINJGOSAUZQCVERBKD
UDEHRLSJNKMYOGPQTBAVCWXZIF
VLXYZJQIONGKSPAUCFTEWRBDMH
WYZIFKTNPGSMAQUCELVRXBDHOJ
XIFNLMVGQSAOUTCERYWBZDHJPK
YANUGTFCXERVBZDHJSLKIMOPWQ
ZNLGYOWSTAUPCVERBIXDFHJKQM

The fully reconstructed key table is

	plaintext letters
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	YANUGTFCXERVBZDHJSLKIMOPWQ
k_2	OWQXTRKZHFLBYJINGVMSPAUCDE
k_3	EJBKDIUMSOPNQATVWHCXRZFLGY
k_4	FGYSIPXAVUCQEWRBDNZHLJKMTO
k_5	ZNLGYOWSTAUPCVERBIXDFHJKQM
k_6	QZVFWDOLKYIHNMGSAXPUTCERJB

Had we only used the first forty-three letters as our crib, we would only have been able to reconstruct this much of the key table:

	plaintext letters
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	Y..UGTF.X.RV.ZDH.SLKIMOPWQ
k_2	O..XTRKZH.L.Y.INGVMSPAU.DE
k_3	EJ.KDIUMS.PNQATVWH.XRZFLGY
k_4	F..SIPXAV..QEWR.DNZHL.KMTO
k_5	Z..GYOWST.UP.VER.IXDFH.KQM
k_6	Q..FWDOLK.IHNMGSAXPUT.ER..

While not perfect, it is still a very good result.

Key amplification in quagmire 4

It is possible to expand our knowledge of the permutations in the key table by looking at differences between rows, remembering that in the original table (where k_P appears in place of the plaintext alphabet) for the cipher contains rows that are rotated versions of k_C [21]. In the following, we look at how the group structure of the Q3 ciphers that are related to the Q4 can be used.

Recall that if we take two elements from $Q_4\,[k_P, k_C]$, say k_1 and k_2, we obtain an element of $Q_3\,[k_P]$ by taking the composition $k_1^{-1} \circ k_2$, and an element of $Q_3\,[k_C]$ by taking the composition $k_2 \circ k_1^{-1}$. Our strategy for key amplification in the Q4 is to take such compositions to find elements of the two associated Q3 tableaux, and to reconstruct those two tableaux as much as possible with the tools of the previous section of this article. Knowledge will pass from one Q3 to the other via the Q4 tableau. If we automate the process, then we focus on one Q3, use what we learn to fill in missing letters in the Q4, then use that new knowledge to improve the other Q3; focus will move across the three tableaux until it is no longer possible to glean any more missing letters. Because the quagmire 4 keys are a shift key and two alphabetic permutations, we require more information to reconstruct the tableau than we needed for the other quagmires.

As expected, we now work an example. Here we have a ciphertext encrypted with a quagmire 4 with period six:

```
KBZFPH APGKFR LCRBQM UMOKUN FIOAYQ FVOGAQ ARAMPN JXOWPW
KKVTPN FPQCDS OKAMUQ IBQAEH OZRBUN MNKWSS ULXBPN BVKFEV
BBJBQK WVTFDW BUTLPN RCJLAW OKODDS OXYGVQ OXUCPI OZYRAI
OUKIFM NBEFDS OKKIGW KFMIUW XKVBGQ UUCBXR WBMWDS UWQXYX
JBMISE KAODVQ FIOCKW VCJTAU FWBEXW XSBKXI QLTBEF UEVGTQ
OUYRXI OZBGAX ANGCYQ OTKFKM FIKQUV VBJTHF UTTLFI NAQHDM
KWJBDS UKQGVQ JCBWSX USAHAW NKVGDQ ISQQYN XTMADM CUHEVR
XEZUHD ISABA
```

Since we need more material, let us try the first eleven groups of letters of the plaintext as crib:

```
NOONEW OULDHA VEBELI EVEDIN THELAS TYEARS OFTHEN INETEE NTHCEN TURYTH ATTHIS
KBZFPH APGKFR LCRBQM UMOKUN FIOAYQ FVOGAQ ARAMPN JXOWPW KKVTPN FPQCDS OKAMUQ
```

From this crib we know this much of the key table:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	O	.	.	.	U	.	.	.	J	.	.	.	.	K	A	.	.	.	.	F	.	L	.	.	.	.
k_2	.	.	.	.	C	R	.	I	.	.	.	.	.	X	B	.	.	.	.	K	P	M	.	.	V	.
k_3	.	R	.	.	O	.	.	V	.	.	.	G	.	.	Z	.	.	Q	.	A	.	.	.	.	.	.
k_4	G	.	T	K	B	.	.	M	.	.	.	A	.	F	.	.	.	.	.	W	.	.	.	.	C	.
k_5	Y	.	.	.	P	.	.	F	U	.	.	Q	.	.	.	.	.	A	.	D	.	.	.	.	.	.
k_6	R	.	.	.	W	.	.	S	M	.	.	.	.	N	.	.	.	.	Q	.	.	.	H	.	.	.

So that we can make a comparison later, we decrypt the remainder of the ciphertext with only the parts of the keys found from the crib directly:

```
NOONEWOULDHAVEBELIEVEDINTHELASTYEARSOFTHENINETEENTHCENTURYT
HATTHIS.ORL.WA.BEIN...T.HE..EEN.Y.N...O.EL..Y.NTE....EN.E..
REATE.THAN.A.SAN.YE.A...R.A...HI.O.NTHAT...EN...IE.THE.SE..
E.A.O.TTHE.R.A.IO....N.E..STHEY.E.E.CR.T....E...D.....E..E.
```

```
HA.SA.....A..AR.O.LYASA..N.ITH..I..O.C..E...H...R.TIN..ETHE
TRA.SIE.T..E.T.RE.THATS..R.AN...LTI.....A..O.....TER
```

Using all combinations of $k_i^{-1} \circ k_j$ using the partial permutations in the key table, we get this partial tableau for $Q_3[k_P]$:

```
      plaintext letters
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
ABCDEFGHIJKLMNOPQRSTUVWXYZ
B.................R.......
E.............T...........
F.......V.................
L..........T..............
.A...............S........
.F.....Y..................
...N.......O.T............
...TO..V................E.
....A..............O......
....I.........R....H......
....T...H.................
....U.....................
....Y.........E....D.H....
.....A...............I....
.....B..................H.
.......I...........E......
.......N.........L.R......
.......TE........O........
...........A.......L......
...........R.H...T........
...........S..............
.............DL....N......
..................L.......
....................E.....
```

After undergoing the procedure from the previous section, we can add some letters and rows to this tableau. Some of the rows are duplicates; we simply do not know yet which can be merged.

```
      plaintext letters
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
ABCDEFGHIJKLMNOPQRSTUVWXYZ
B.................R.......
E...D......N..T..H........
F.......V...............T.
L...N......T..............
```

```
.A...............S........
.F.....Y.............E....
...NL......O.T............
...TO..VR.....F.........E.
...EA..R.....L.....O......
....I.........R..N.H......
O...T...H........V......D.
....U.....................
....YO........E..I.D.H....
.....A.............Y.I....
....VB..................H.
...Y...I......A....E.R....
...I...N.........L.R......
.......TE....R...O........
...........A.E.....L......
........D..R.H...T........
...........S..............
...........E.DL....N......
..................L.......
....................E.....
I....V........H...........
R...H.........V...........
SR........................
Y....T........D...........
.H...Y....................
.V...E........Y...........
...HR...N..........V....I.
...L.........O............
...O...............F....A.
...R....L.................
....F................B..O.
.....L.....Y..............
.....R........I...........
.......B................F.
.......DY....I...E...T....
.......E.........A...O....
.......OA............F....
........O........F........
........T....V............
...........D..N...........
...........F............L.
...........I.....D........
.................BA.......
.................Y...D....
...................I.N....
```

We bring them back to the Q4 by composing each of these on the left with k_1, ..., k_6. After we merge the results into the Q4 key table we find some new letters:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	O	.	.	X	U	.	.	.	J	.	.	B	.	K	A	.	.	V	.	F	.	L	.	.	.	.
k_2	.	.	.	.	C	R	.	I	.	.	.	U	.	X	B	.	.	.	.	K	P	M	.	.	V	.
k_3	.	R	.	U	O	.	.	V	.	.	.	G	.	B	Z	.	.	Q	.	A	.	C	.	.	.	.
k_4	G	.	T	K	B	.	.	M	.	.	.	A	.	F	R	.	.	D	.	W	.	.	.	.	C	.
k_5	Y	.	.	.	P	.	.	F	U	.	.	Q	.	V	.	.	.	A	.	D	.	.	.	.	.	.
k_6	R	.	.	.	W	.	.	S	M	.	.	.	.	N	.	.	.	.	Q	.	.	.	H	.	K	.

We then repeat the process for $Q_3[k_C]$, by using what we now know about the Q4 key table. And then back to the $Q_3[k_P]$. After a very long and tedious process, we finally reach the point at which no new knowledge can be extracted. At this point the key table looks like this:

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	O	W	.	X	U	.	.	.	J	.	.	B	.	K	A	.	.	V	.	F	Q	L	.	.	D	.
k_2	.	F	.	L	C	R	.	I	W	.	.	U	.	X	B	.	.	.	Z	K	P	M	.	.	V	.
k_3	.	R	.	U	O	.	.	V	.	.	.	G	.	B	Z	.	.	Q	.	A	.	C	.	.	.	.
k_4	G	J	T	K	B	P	.	M	.	.	.	A	.	F	R	.	.	D	.	W	.	X	.	.	C	.
k_5	Y	C	.	.	P	O	.	F	U	.	.	Q	.	V	.	.	.	A	.	D	Z	J	.	.	R	.
k_6	R	.	.	.	W	D	.	S	M	.	.	J	.	N	.	.	.	X	Q	I	U	.	H	.	K	.

We see definite improvement, from about 30% knowledge of the key table to about 50%. For comparison, we can decrypt the full text with this new knowledge:

```
NOONEWOULDHAVEBELIEVEDINTHELASTYEARSOFTHENINETEENTHCENTURYT
HATTHIS.ORL.WASBEIN...T.HED.EENLY.N..LO.ELYBY.NTELL..EN.E..
REATERTHAN.ANSANDYETAS.ORTAL..HI.O.NTHAT...ENB..IEDTHE.SELV
E.ABO.TTHEIRVARIO....N.ERNSTHEY.ERE.CRUTIN..ED.ND.TUD.E..E.
HA.SAL.O.TASNARRO.LYASA..N.ITH..I.RO.C..E...HT..R.TINI.ETHE
TRANSIENT.RE.T.RE.THATS..R.AND..LTI.L..NAD.O..F..TER
```

With more crib material, we can do better. With ninety letters of crib, we get

	plaintext letters																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k_1	O	W	R	X	U	T	M	Y	J	.	S	B	.	K	A	.	.	V	N	F	Q	L	I	.	D	.
k_2	S	F	A	L	C	R	Y	I	W	.	H	U	.	X	B	.	.	E	Z	K	P	M	N	.	V	.
k_3	K	R	N	U	O	I	D	V	T	.	X	G	.	B	Z	.	.	Q	J	A	M	C	E	.	H	.
k_4	G	J	T	K	B	P	L	M	E	.	O	A	.	F	R	.	.	D	I	W	H	X	Y	.	C	.

k_5	Y C S E P O W F U . I Q . V H . . A X D Z J K . R .
k_6	R Y V Z W D O S M . A J . N E . . X Q I U G H . K .

And we can see how the resulting decryption is improved:

```
NOONEWOULDHAVEBELIEVEDINTHELASTYEARSOFTHENINETEENTHCENTURYT
HATTHISWORLDWASBEINGWATCHEDKEENLYANDCLOSELYBYINTELLIGENCESG
REATERTHAN.ANSANDYETAS.ORTALASHISOWNTHATAS.ENBUSIEDTHE.SELV
ESABOUTTHEIRVARIOUSCONCERNSTHEYWERESCRUTINISEDANDSTUDIED.ER
HA.SAL.OSTASNARROWLYASA.ANWITHA.ICROSCO.E.IGHTSCRUTINISETHE
TRANSIENTCREATURESTHATSWAR.AND.ULTI.LYINADRO.OFWATER
```

Application: identification of the cipher

For this and the next application, we assume that we have (nearly) completely reconstructed the key table, or at least two distinct permutations in it (call them k_1 and k_2). Here we discuss clues to the identification of the cipher; later we discuss keyword recovery.

If the column property does not hold, i.e., there is a column in the key table in which a letter appears more than once but in distinct permutations, then the cipher is not in the quagmire family. While otherwise we are not guaranteed to have a quagmire, we will assume that we have for the following tests.

If the cipher is one of Vigenère, Beaufort, or Porta/Bellaso, then we should immediately recognize the permutations as belonging to the appropriate tableau, since those tableaux are fixed. For example, all permutations of the Vigenère are rotations.

All permutations of a quagmire 1 have the form $R_n \circ k^{-1}$ for base key k. Therefore, we can test for Q1 by taking $k_1 \circ k_2^{-1}$ and looking for a rotation:

$$k_1 \circ k_2^{-1} \;=\; (R_m \circ k^{-1}) \circ (R_n \circ k^{-1})^{\,-1} = \; R_m \circ k^{-1} \circ k \circ R_{-n} \;=\; R_m \circ e \circ R_{-n} \;=\; R_m \circ R_{-n} \;=\; R_{m-n}$$

The permutations of a quagmire 2 are of the form $k \circ R_n$ for base key k. So in this case, we can test for Q2 by taking $k_1^{-1} \circ k_2$ and looking for a rotation:

$$k_1^{-1} \circ k_2 \;=\; (k \circ R_m)^{-1} \circ (k \circ R_n) \;=\; R_{-m} \circ k^{-1} \circ k \circ R_n \;=\; R_{-m} \circ e \circ R_n \;=\; R_{-m} \circ R_n \;=\; R_{n-m}$$

If we have not yet identified the cipher by any of the above tests, then we find the order of the permutations. If they are both 1, 2, 13, or 26 (not necessarily the same), then we are confident that we have a quagmire 3. We can be even more confident if we find that one of them is in the orbit of the other; in other words, if we can find an n such that

$$k_1^{\,n} \;=\; k_2$$

Be aware that in a cyclic group like Q3, such an n can be found only if the order of k_1 is larger or equal to the order of k_2.

If all of the above tests have failed, then we look at $k_1 \circ k_2^{-1}$ and $k_1^{-1} \circ k_2$. If they both pass the Q3 tests, then the cipher is most likely quagmire 4.

Application: keyword recovery

The keys of the polyalphabetic substitution ciphers in the Vigenère-quagmire family are typically specified by a set of keywords. The keyword that we call a “shift key” specifies the rows of the tableau that are used to encipher the text. This is the only key needed for the Vigenère and Beaufort ciphers. For the quagmires, we also need one or two additional keywords, from which the base keys are formed. Our favorite example uses the keyword `FLYINGSAUCER`, to form this base key:

$$k = \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

In the next few sections, we explain how to recover the keywords from the (completely filled) key table. We begin with the easier ciphers and work our way to the quagmire 3 and 4.

Keyword recovery in the Vigenère cipher

The Vigenère is a trivially easy cipher for keyword recovery, once the key table is known. The shift keyword appears in the leftmost column of the table. From our earlier example:

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_2	LMNOPQRSTUVWXYZABCDEFGHIJK
k_3	IJKLMNOPQRSTUVWXYZABCDEFGH
k_4	EFGHIJKLMNOPQRSTUVWXYZABCD
k_5	NOPQRSTUVWXYZABCDEFGHIJKLM

Keyword recovery in quagmire 2

With a quagmire 2 key table, finding the keywords is also easy. The shift key appears in the first column, and since every permutation is a rotation of the base key, we can see the keyword immediately. For example, here is the key table from our example above regarding key amplification:

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	TVWXZFLYINGSAUCERBDHJKMOPQ
k_2	RBDHJKMOPQTVWXZFLYINGSAUCE
k_3	INGSAUCERBDHJKMOPQTVWXZFLY
k_4	PQTVWXZFLYINGSAUCERBDHJKMO
k_5	OPQTVWXZFLYINGSAUCERBDHJKM
k_6	DHJKMOPQTVWXZFLYINGSAUCERB

Keyword recovery in quagmire 1

Recall that the permutations of a Q1 cipher have the form $R_n \circ k^{-1}$, and that if we invert them we have permutations of the form $k \circ R_{-n}$. We will therefore find the shift key in the first column of the key table, but the alphabetic keyword in the inverse permutations.

Here is the key table from our example for key amplification. The shift key is in the first column:

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	TYVZWMRAPBCNDQEFGXSHUIJKOL
k_2	RWTXUKPYNZALBOCDEVQFSGHIMJ
k_3	INKOLBGPEQRCSFTUVMHWJXYZDA
k_4	PURVSINWLXYJZMABCTODQEFGKH
k_5	OTQURHMVKWXIYLZABSNCPDEFJG
k_6	DIFJGWBKZLMXNAOPQHCRESTUYV

Here are the inverses, from which we readily see the other keyword:

k_1^{-1}	HJKMOPQTVWXZFLYINGSAUCERBD
k_2^{-1}	KMOPQTVWXZFLYINGSAUCERBDHJ
k_3^{-1}	ZFLYINGSAUCERBDHJKMOPQTVWX
k_4^{-1}	OPQTVWXZFLYINGSAUCERBDHJKM
k_5^{-1}	PQTVWXZFLYINGSAUCERBDHJKMO
k_6^{-1}	NGSAUCERBDHJKMOPQTVWXZFLYI

Keyword recovery in quagmire 3 with an element of order 26

Before we get to the complicated parts, let us first consider the shift key. The shift key is found in a column of the key table, but not necessarily the first. The plaintext letter under which it appears is the first letter of the base key. Looking at the key table from our key-amplification example, we see the shift key `TRIPOD` under the letter `F`:

	plaintext letters ABCDEFGHIJKLMNOPQRSTUVWXYZ	order
k_1	YANUGTFCXERVBZDHJSLKIMOPWQ	26
k_2	OWQXTRKZHFLBYJINGVMSPAUCDE	26
k_3	EJBKDIUMSOPNQATVWHCXRZFLGY	26
k_4	FGYSIPXAVUCQEWRBDNZHLJKMTO	26
k_5	ZNLGYOWSTAUPCVERBIXDFHJKQM	13
k_6	QZVFWDOLKYIHNMGSAXPUTCERJB	2

Automating the search for the shift key is possible if that key is a recognizably English word or set of words, and we have the ability to discriminate good from bad text. Knowing with which letter to begin the base key is useful, as we will see below, where we do examples in which we do not know it a priori.

Gains [1] has a method for finding the base key from an order-26 element of the Q3 tableau. She first rewrites the permutation as a 26-cycle. If the keyword is not apparent, she then takes every third letter of the cycle, or every fifth letter, etc., but *not* every thirteenth. These choices should look familiar to us, as they avoid the factors of 26 = 2·13. Let us see the process in action with k_1 from our key table. Written as a cycle, it is

$$k_1 = (\mathtt{AYWODUIXPHCNZQJEGFTKRSLVMB})$$

We know from above that the base key begins with F, so we can rewrite the cycle beginning with that letter:

$$k_1 = (\mathtt{FTKRSLVMBAYWODUIXPHCNZQJEG})$$

Writing every n^{th} letter of this cycle gives us these possibilities:

n	
1	FTKRSLVMBAYWODUIXPHCNZQJEG
3	FRVAOIHZETSMYDXCQGKLBWUPNJ
5	FLYINGSAUCERBDHJKMOPQTVWXZ
7	FMUZKAXJSWHGVDNTBIQRYPELOC
9	FAHTYCKWNROZSDQLUJVIEMXGBP
11	FWQMHRUGYZVPKDEANLXTOJBCSI
15	FISCBJOTXLNAEDKPVZYGURHMQW
17	FPBGXMEIVJULQDSZORNWKCYTHA
19	FCOLEPYRQIBTNDVGHWSJXAKZUM
21	FZXWVTQPOMKJHDBRECUASGNIYL
23	FJNPUWBLKGQCXDYMSTEZHIOAVR
25	FGEJQZNCHPXIUDOWYABMVLSRKT

And we have found the base key when $n = 5$.

To see why this method works, we look back on the original way in which the Q3 cipher is implemented. The plaintext alphabet across the top of the table is deranged according to the base key, and each row in the table is a rotated version of the base key. For our example we only write three of the rows here:

	plaintext letters
	FLYINGSAUCERBDHJKMOPQTVWXZ
$k \circ R_1$	LYINGSAUCERBDHJKMOPQTVWXZF
$k \circ R_3$	INGSAUCERBDHJKMOPQTVWXZFLY
$k \circ R_{21}$	TVWXZFLYINGSAUCERBDHJKMOPQ

Enciphering with the first row takes F → L, L → Y, Y → I, etc. This row gives us the cycle

(FLYINGSAUCERBDHJKMOPQTVWXZ)

The third row takes F → I, I → S, S → C, etc., giving us this cycle, which runs across every third letter in the base key:

(FISCBJOTXLNAEDKPVZYGURHMQW)

The third row runs across every twenty-first letter:

(FTKRSLVMBAYWODUIXPHCNZQJEG)

This is the cycle for k_1 from our key table. Taking every fifth letter of it gives the base key, since $21^{-1} = 5$ modulo 26. The reason that we have to take every n^{th} letter, for the invertible values of n, is that we have chosen to work with an order-26 member of the set $\mathcal{Q}_3[k]$, but we do not know which one. Taking every n^{th} letter is the equivalent of applying one of the automorphisms of $(\mathcal{V}, \circ)$, which as we recall, were the permutations of the multiplication cipher $\{M_m\}$, which take R_1 to R_m, so there is a corresponding automorphism of $(\mathcal{Q}_3[k], \circ)$ that takes $k \circ R_1 \circ k^{-1}$ to $k \circ R_m \circ k^{-1}$.

Now let us investigate a more group-theoretic way to find the base key from an order-26 permutation. The order-26 permutation (call it $q_{[26]}$) is of the form $k \circ R_n \circ k^{-1}$, where n is one of the invertible numbers modulo 26, and we do not yet know the base key k or the value of n. Because of the automorphisms mentioned above, we can assume that $n = 1$ provisionally, and make the correction later. So what we need to do is find a transformation k' that maps R_1 to our order-26 permutation:

$$R_1 \rightarrow k' \circ R_1 \circ k'^{-1} = q_{[26]} = k \circ R_n \circ k^{-1}$$

The base key k and provisional key k' are related by one of the automorphisms:

$$\begin{aligned} k \circ R_n \circ k^{-1} &= k \circ (M_n \circ R_1 \circ M_n^{-1}) \circ k^{-1} \\ &= (k \circ M_n) \circ R_1 \circ (M_n^{-1} \circ k^{-1}) \\ &= (k \circ M_n) \circ R_1 \circ (k \circ M_n^{-1})^{-1} \end{aligned}$$

so that

$$k' = k \circ M_n$$

Thus, if we can find a provisional base key under the assumption that our order-26 permutation was built from R_1, then we can find the true base key among the twelve possibilities

$$k = k' \circ M_n^{-1}$$

where n is 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, or 25.

The question is then how to find the provisional base key. We state without proving that any permutation can be found as a product of exchanges. An exchange is a permutation that simply swaps two items, i.e., a 2-cycle. For example, the exchange that swaps the first two letters is

$$E_{0,1} \;=\; \texttt{BACDEFGHIJKLMNOPQRSTUVWXYZ} \;=\; \texttt{(AB)}$$

Whereas before we saw that the order-2 permutations were products of disjoint 2-cycles, here the 2-cycles will be overlapping when we form the product. Since any permutation is a product of exchanges, we can get from the identity permutation to any other permutation by a series of exchanges. Therefore, we can get from any permutation to any other by a series of exchanges; one possible series takes us from one to the identity and then to the other. With alphabetic permutations, we can get from one to another with twenty-five or fewer steps. Our strategy then is to find a series of exchanges that takes $q_{[26]}$ to R_1. The product of those exchanges is k'. To be clear, every time we act with an exchange, we must do so from the left, and also apply its inverse on the right. Since exchanges are self-reciprocal, the inverse of an exchange is itself. What we are saying is

$$q_{[26]} \;=\; E_{ij} \circ \ldots \circ E_{cd} \circ E_{ab} \circ R_1 \circ E_{ab} \circ E_{cd} \circ \ldots \circ E_{ij}$$

and

$$k' \;=\; E_{ij} \circ \ldots \circ E_{cd} \circ E_{ab}$$

Because of the application of the exchanges to both sides, each will move more that two letters. Therefore it is practical to start at the beginning of the permutation and work our way to the end. In practice, it is easier to go from $q_{[26]}$ to R_1 and then invert the order of the exchanges. The example below will make this more clear. Also, a mathematician may prefer to diagonalize some matrices as an alternative method to find k'.

Return to our example permutation from the Q3 key table:

$$q_{[26]} \;=\; \texttt{YANUGTFCXERVBZDHJSLKIMOPWQ}$$

Here is a series of exchanges that transforms it to R_1:

$q_{[26]}$ =	YANUGTFCXERVBZDHJSLKIMOPWQ	
→	BWNUGTFCXERVYZDHJSLKIMOPAQ	$E_{1,24}$
→	BCOUGTFWXERVYZDHJSLKIMNPAQ	$E_{2,22}$
→	BCDOGTFWXERVYZUHJSLKIMNPAQ	$E_{3,14}$
→	BCDEUTFWXORVYZGHJSLKIMNPAQ	$E_{4,14}$
→	BCDEFIUWXORVYZGHJSLKTMNPAQ	$E_{5,20}$
→	BCDEFGXWUORVYZIHJSLKTMNPAQ	$E_{6,8}$
→	BCDEFGHPUORVYZIXJSLKTMNWAQ	$E_{7,23}$
→	BCDEFGHIXORVYZPUJSLKTMNWAQ	$E_{8,15}$
→	BCDEFGHIJWRVYZPUXSLKTMNOAQ	$E_{9,23}$
→	BCDEFGHIJKNVYZPUXSLWTMROAQ	$E_{10,22}$
→	BCDEFGHIJKLZYVPUXSNWTMROAQ	$E_{11,13}$
→	BCDEFGHIJKLMQVPUXSNWTZROAY	$E_{12,25}$
→	BCDEFGHIJKLMNXPUVSQWTZROAY	$E_{13,16}$

$$\begin{array}{lll}
\to & \texttt{BCDEFGHIJKLMNOXUVSQWTZRPAY} & E_{14,23} \\
\to & \texttt{BCDEFGHIJKLMNOPXVSQWTZRUAY} & E_{15,23} \\
\to & \texttt{BCDEFGHIJKLMNOPQUSXWTZRVAY} & E_{16,23} \\
\to & \texttt{BCDEFGHIJKLMNOPQRTXWSZUVAY} & E_{17,20} \\
\to & \texttt{BCDEFGHIJKLMNOPQRSWXTZUVAY} & E_{18,19} \\
\to & \texttt{BCDEFGHIJKLMNOPQRSTUWZXVAY} & E_{19,22} \\
\to & \texttt{BCDEFGHIJKLMNOPQRSTUVXZWAY} & E_{21,22} \\
\to & \texttt{BCDEFGHIJKLMNOPQRSTUVWXZAY} & E_{22,23} \\
\to & \texttt{BCDEFGHIJKLMNOPQRSTUVWXYZA} = R_1 & E_{24,25}
\end{array}$$

The provisional base key is (yes, this is the inverted order)

$$k' = E_{1,24} \circ E_{2,22} \circ E_{3,14} \circ \ldots \circ E_{21,22} \circ E_{22,23} = \texttt{AYWODUIXPHCNZQJEGFTKRSLVMB}$$

The possibilities from which we choose the true base key are

$$\begin{array}{lcl}
k' \circ M_1^{-1} & = & \texttt{AYWODUIXPHCNZQJEGFTKRSLVMB} \\
k' \circ M_3^{-1} & = & \texttt{AHTYCKWNROZSDQLUJVIEMXGBPF} \\
k' \circ M_5^{-1} & = & \texttt{ASGNIYLFZXWVTQPOMKJHDBRECU} \\
k' \circ M_7^{-1} & = & \texttt{AEDKPVZYGURHMQWFISCBJOTXLN} \\
k' \circ M_9^{-1} & = & \texttt{AOIHZETSMYDXCQGKLBWUPNJFRV} \\
k' \circ M_{11}^{-1} & = & \texttt{AKZUMFCOLEPYRQIBTNDVGHWSJX} \\
k' \circ M_{15}^{-1} & = & \texttt{AXJSWHGVDNTBIQRYPELOCFMUZK} \\
k' \circ M_{17}^{-1} & = & \texttt{AVRFJNPUWBLKGQCXDYMSTEZHIO} \\
k' \circ M_{19}^{-1} & = & \texttt{ANLXTOJBCSIFWQMHRUGYZVPKDE} \\
k' \circ M_{21}^{-1} & = & \texttt{AUCERBDHJKMOPQTVWXZFLYINGS} \\
k' \circ M_{23}^{-1} & = & \texttt{AFPBGXMEIVJULQDSZORNWKCYTH} \\
k' \circ M_{25}^{-1} & = & \texttt{ABMVLSRKTFGEJQZNCHPXIUDOWY}
\end{array}$$

At this point, we have to pick out the best one; this can be automated if we discriminate orderly permutations with recognizable words from the others. The best seems to be

$$k'' = k' \circ M_{21}^{-1} = \texttt{AUCERBDHJKMOPQTVWXZFLYINGS}$$

We are almost finished, but first we must mention that a rotation of the base key does not change the set of permutations $Q_3\,[k]$, but it will put them into different rows of the tableau. The resulting cipher is equivalent, although the shift key must be adjusted. We can see that the set of permutations remains the same by considering

$$k \to k \circ R_m$$

Then

$$\begin{aligned}
q_n = k \circ R_n \circ k^{-1} \to \; & (k \circ R_m) \circ R_n \circ (k \circ R_m)^{-1} \\
= \; & k \circ R_m \circ R_n \circ R_{-m} \circ k^{-1} \\
= \; & k \circ R_{n+m-m} \circ k^{-1}
\end{aligned}$$

$$= \; k \circ R_n \circ k^{-1} \; = \; q_n$$

We can harmlessly rotate k'' to obtain k, which begins with `F`, as we know from above that it should. We now have it and the keyword:

$$k \; = \; \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

Keyword recovery in quagmire 3 with an element of order 13

If we start with an order-13 permutation and want to recover the keyword, your first thought might be that we can do so in a way similar to the previous section. However, there are complications.

Gaines [1] explains her method of keyword recovery from an order-13 member of the key table. The permutation is factored into two 13-cycles. The letters of these cycles are interleaved; there are thirteen possibilities here. Then letters are read off every n^{th} one, as we did for the order-26 case; there are twelve possibilities here. The total is 13·12 = 156 possibilities from which we must pick out the keyword. As an example, take k_5 from our Q3 key table. We can call it $q_{[13]}$ if we like.

$$k_5 \; = \; q_{[13]} \; = \; \texttt{ZNLGYOWSTAUPCVERBIXDFHJKQM}$$

Factor it into cycles:

$$q_{[13]} \; = \; (\texttt{AZMCLPRITDGWJ})\,(\texttt{BNVHSXKUFOEYQ})$$

The twelve interleavings are

```
ABZNMVCHLSPXRKIUTFDOGEWYJQ
ANZVMHCSLXPKRUIFTODEGYWQJB
AVZHMSCXLKPURFIOTEDYGQWBJN
AHZSMXCKLUPFROIETYDQGBWNJV
ASZXMKCULFPOREIYTQDBGNWVJH
AXZKMUCFLOPERYIQTBDNGVWHJS
AKZUMFCOLEPYRQIBTNDVGHWSJX
AUZFMOCELYPQRBINTVDHGSWXJK
AFZOMECYLQPBRNIVTHDSGXWKJU
AOZEMYCQLBPNRVIHTSDXGKWUJF
AEZYMQCBLNPVRHISTXDKGUWFJO
AYZQMBCNLVPHRSIXTKDUGFWOJE
AQZBMNCVLHPSRXIKTUDFGOWEJY
```

With hindsight we say that the seventh one is the best choice. Taking every n^{th} letter from the seventh interleaving gives these twelve possibilities. The keyword is apparent for n = 3.

n	
1	AKZUMFCOLEPYRQIBTNDVGHWSJX
3	AUCERBDHJKMOPQTVWXZFLYINGS
5	AFPBGXMEIVJULQDSZORNWKCYTH
7	AOIHZETSMYDXCQGKLBWUPNJFRV
9	AEDKPVZYGURHMQWFISCBJOTXLN
11	AYWODUIXPHCNZQJEGFTKRSLVMB
15	ABMVLSRKTFGEJQZNCHPXIUDOWY
17	ANLXTOJBCSIFWQMHRUGYZVPKDE
19	AVRFJNPUWBLKGQCXDYMSTEZHIO
21	AHTYCKWNROZSDQLUJVIEMXGBPF
23	ASGNIYLFZXWVTQPOMKJHDBRECU
25	AXJSWHGVDNTBIQRYPELOCFMUZK

Now we shall look at the problem through the group theorist's lenses. In parallel to the previous section, we will want to find a transformation between $q_{[13]}$ of the Q3 tableau and R_2 of the Vigenère tableau. But then the complications come in. The order-13 members, together with the order-1 member, of either of these groups form a subgroup that is isomorphic to ($\mathbb{Z}_{13}$, + mod 13). This means that no matter how we combine them, group closure guarantees that we cannot obtain a permutation with order 26.

As an aside, we mention that there is another subgroup of ($\mathcal{V}$, $\circ$), and hence also of ($Q_3[k]$, $\circ$). Its set consists of the order-1 and order-2 elements. In ($\mathcal{V}$, $\circ$) that subset is ($\{R_0, R_{13}\}$, $\circ$). It is isomorphic to ($\mathbb{Z}_2$, + mod 2). There are $12!{\cdot}2^{12}$ quagmire 3 groups that overlap this subgroup of ($\mathcal{V}$, $\circ$), and for this reason, keyword recovery from an order-2 permutation alone is not feasible.

We can solve our problem with $q_{[13]}$ if we can find something like a "square root" of R_2, i.e., some permutation X such that

$$X \circ X = R_2$$

The difficulty is that there are thirteen of them. Each of them has order 26 and generates a ($Q_3[X]$, $\circ$) that contains the same subgroup ($\{R_0, R_2, R_4, ..., R_{24}\}$, $\circ$) of ($\mathcal{V}$, $\circ$). We will now see how to construct them. Consider these thirteen permutations:

D_0 = ABCDEFGHIJKLMNOPQRSTUVWXYZ = e
D_1 = ADCFEHGJILKNMPORQTSVUXWZYB
D_2 = AFCHEJGLINKPMROTQVSXUZWBYD
D_3 = AHCJELGNIPKRMTOVQXSZUBWDYF
D_4 = AJCLENGPIRKTMVOXQZSBUDWFYH
D_5 = ALCNEPGRITKVMXOZQBSDUFWHYJ
D_6 = ANCPERGTIVKXMZOBQDSFUHWJYL
D_7 = APCRETGVIXKZMBODQFSHUJWLYN = D_6^{-1}
D_8 = ARCTEVGXIZKBMDOFQHSJULWNYP = D_5^{-1}

$$\begin{aligned}
D_9 &= \texttt{ATCVEXGZIBKDMFOHQJSLUNWPYR} = D_4^{-1}\\
D_{10} &= \texttt{AVCXEZGBIDKFMHOJQLSNUPWRYT} = D_3^{-1}\\
D_{11} &= \texttt{AXCZEBGDIFKHMJOLQNSPURWTYV} = D_2^{-1}\\
D_{12} &= \texttt{AZCBEDGFIHKJMLONQPSRUTWVYX} = D_1^{-1}
\end{aligned}$$

They share the same interleaving pattern we saw above. $(\{D_n\}, \circ)$ forms its own group isomorphic to $(\mathbb{Z}_{13}, + \bmod 13)$:

$$D_m \circ D_n = D_{m+n}$$

where the addition in the subscript is done modulo 13. We use these D_n to transform R_1 into a generator of a $(Q_3\,[D_n], \circ)$ that contains R_2. For example,

$$X = D_3 \circ R_1 \circ D_3^{-1} = \texttt{HWJYLANCPERGTIVKXMZOBQDSFU}$$

This permutation generates the quagmire 3 that has these members:

$$\begin{aligned}
X &= \texttt{HWJYLANCPERGTIVKXMZOBQDSFU}\\
X^2 &= \texttt{CDEFGHIJKLMNOPQRSTUVWXYZAB} = R_2\\
X^3 &= \texttt{JYLANCPERGTIVKXMZOBQDSFUHW}\\
X^4 &= \texttt{EFGHIJKLMNOPQRSTUVWXYZABCD} = R_4\\
X^5 &= \texttt{LANCPERGTIVKXMZOBQDSFUHWJY}\\
X^6 &= \texttt{GHIJKLMNOPQRSTUVWXYZABCDEF} = R_6\\
X^7 &= \texttt{NCPERGTIVKXMZOBQDSFUHWJYLA}\\
X^8 &= \texttt{IJKLMNOPQRSTUVWXYZABCDEFGH} = R_8\\
X^9 &= \texttt{PERGTIVKXMZOBQDSFUHWJYLANC}\\
X^{10} &= \texttt{KLMNOPQRSTUVWXYZABCDEFGHIJ} = R_{10}\\
X^{11} &= \texttt{RGTIVKXMZOBQDSFUHWJYLANCPE}\\
X^{12} &= \texttt{MNOPQRSTUVWXYZABCDEFGHIJKL} = R_{12}\\
X^{13} &= \texttt{TIVKXMZOBQDSFUHWJYLANCPERG}\\
X^{14} &= \texttt{OPQRSTUVWXYZABCDEFGHIJKLMN} = R_{14}\\
X^{15} &= \texttt{VKXMZOBQDSFUHWJYLANCPERGTI}\\
X^{16} &= \texttt{QRSTUVWXYZABCDEFGHIJKLMNOP} = R_{16}\\
X^{17} &= \texttt{XMZOBQDSFUHWJYLANCPERGTIVK}\\
X^{18} &= \texttt{STUVWXYZABCDEFGHIJKLMNOPQR} = R_{18}\\
X^{19} &= \texttt{ZOBQDSFUHWJYLANCPERGTIVKXM}\\
X^{20} &= \texttt{UVWXYZABCDEFGHIJKLMNOPQRST} = R_{20}\\
X^{21} &= \texttt{BQDSFUHWJYLANCPERGTIVKXMZO}\\
X^{22} &= \texttt{WXYZABCDEFGHIJKLMNOPQRSTUV} = R_{22}\\
X^{23} &= \texttt{DSFUHWJYLANCPERGTIVKXMZOBQ}\\
X^{24} &= \texttt{YZABCDEFGHIJKLMNOPQRSTUVWX} = R_{24}\\
X^{25} &= \texttt{FUHWJYLANCPERGTIVKXMZOBQDS}\\
X^{26} &= \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} = R_0
\end{aligned}$$

The members that overlap the Vigenère set have been noted. They are exactly the ones in the subgroup isomorphic to $(\mathbb{Z}_{13}, + \bmod 13)$.

The strategy for keyword recovery is to find, by whatever means is easiest, a provisional base key k' that transforms R_2 to $q_{[13]}$:

$$q_{[13]} \;=\; k' \circ R_2 \circ k'^{-1}$$

Since we do not know which of the thirteen Q3 ciphers $k' \circ R_1 \circ k'^{-1}$ will land in, we must compose with each of the D_n^{-1} on the right. Then, since we also have a twelve order-26 rotations that can stand in for R_1, we have to take into account the twelve possible automorphisms of $(\mathcal{V}, \circ)$ by trying each of the M_m and composing on the right. In the end, there may be a harmless rotation, so add an R_r to the mix:

$$k \;=\; k' \circ D_n^{-1} \circ M_m^{-1} \circ R_r$$

Before the final rotation, we have 12·13 = 156 possibilities to examine.

We have an order-13 permutation in our example key table:

$$q_{[13]} \;=\; k_5 \;=\; \texttt{ZNLGYOWSTAUPCVERBIXDFHJKQM}$$

A series of exchanges that take us between $q_{[13]}$ and R_2 is

$$\begin{aligned} k' \;=\; & E_{2,25} \circ E_{3,13} \circ E_{4,12} \circ E_{5,21} \circ E_{6,25} \circ E_{8,11} \circ E_{9,18} \circ E_{10,15} \circ E_{11,23} \circ E_{12,17} \circ \\ & E_{13,15} \circ E_{14,23} \circ E_{15,20} \circ E_{16,19} \circ E_{17,21} \circ E_{18,20} \circ E_{19,23} \circ E_{20,25} \circ E_{23,24} \circ E_{24,25} \\ =\; & \texttt{ABZNMVCHLSPXRKIUTFDOGEWYJQ} \end{aligned}$$

Having already solved this proble, we say with hindsight that the correct D_n is D_7. So

$$k'' \;=\; k' \circ D_7^{-1} \;=\; \texttt{AKZUMFCOLEPYRQIBTNDVGHWSJX}$$

The best M_m to use is M_9:

$$k''' \;=\; k'' \circ M_9^{-1} \;=\; \texttt{AUCERBDHJKMOPQTVWXZFLYINGS}$$

And a final rotation gives us the base key:

$$k \;=\; k''' \circ R_{19} \;=\; \texttt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

Having an order-26 permutation makes keyword recovery relatively easy. If one is not present in our key table, an order-13 element is also usable, even if not as easily. The presence of both an order-13 permutation and the order-2 permutation, however, allows us to construct an order-26 permutation by composing the two. For example, in our key table above, the composition of the last two rows is

$$k_5 \circ k_6 \;=\; \texttt{BMHOJGEPUQTSVCWXZKRFDLYIAN}$$

which has order 26. Another way to understand this is to consider the thirteen different quagmire 3 sets that contain the order-13 element. Finding the one that also contains the order-2 element allows us to pick out the correct Q3.

Keyword recovery in quagmire 4

Gaines [1] also has a method for finding the keywords of a quagmire 4 cipher. Because there are two keywords, it requires two permutations from the key table. In the original Q4 table, the plaintext alphabet across the top was still mixed with k_P, and the rows were rotated versions of k_C. Therefore, between two rows there is a constant shift. So we can find cycle(s) by chaining letters from one row to another. This does not change after we shuffle the columns of the table to straighten out the plaintext alphabet. This will give us a provisional k_C. Then, k_P is found by comparing to the plaintext alphabet.

Consider our example key table:

	plaintext letters
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	OWRXUTMYJZSBPKACEVNFQLIGDH
k_2	SFALCRYIWGHUTXBDJEZKPMNOVQ
k_3	KRNUOIDVTWXGYBZSPQJAMCEFHL
k_4	GJTKBPLMENOAQFRUVDIWHXYZCS
k_5	YCSEPOWFULIQGVHTBAXDZJKMRN
k_6	RYVZWDOSMPAJCNEFLXQIUGHTKB

Focus on k_1 and k_2:

```
OWRXUTMYJZSBPKACEVNFQLIGDH
SFALCRYIWGHUTXBDJEZKPMNOVQ
```

Cycle(s) are formed by taking columns, O → S, W → F, R → A, etc. We obtain one 26-cycles, which forms our provisional base key k_C':

k_C' = (ABUCDVEJWFKXLMYINZGOSHQPTR)

Taking every third letter in this cycle gives

k_C = ACEFLIGHTBDJKMNOQRUVWXYZSP

To recover the other keyword, recall that in the original table for a Q4, the mixed plaintext alphabet (k_P) is written across the top, and rotated versions of k_C appear in the rows. So if we put the straight alphabet above k_1:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
OWRXUTMYJZSBPKACEVNFQLIGDH
```

and rearrange the columns so that the lower row becomes k_C:

```
OPQTVWXZFLYINGSAUCERBDHJKM
ACEFLIGHTBDJKMNOQRUVWXYZSP
```

then the upper row reveals k_P. This is equivalent to finding $k_1^{-1} \circ k_C$. (We have ignored some rotations.)

Now let us do it in a way that exploits the structure of a quagmire 4 cipher, in particular the fact that it is a right coset and left coset of two quagmire 3 sets. We need two permutations from its tableau; call them q_1 and q_2. There are numbers m and n in 0, 1, 2, ..., 25 such that

$$\begin{aligned} q_1 &= k_\mathrm{C} \circ R_m \circ k_\mathrm{P}^{-1} \\ q_2 &= k_\mathrm{C} \circ R_n \circ k_\mathrm{P}^{-1} \end{aligned}$$

where k_P and k_C are the base keys of the Q4. Then

$$\begin{aligned} q_1^{-1} \circ q_2 &= (k_\mathrm{C} \circ R_m \circ k_\mathrm{P}^{-1})^{-1} \circ (k_\mathrm{C} \circ R_n \circ k_\mathrm{P}^{-1}) \\ &= k_\mathrm{P} \circ R_{-m} \circ k_\mathrm{C}^{-1} \circ k_\mathrm{C} \circ R_n \circ k_\mathrm{P}^{-1} \\ &= k_\mathrm{P} \circ R_{-m} \circ e \circ R_n \circ k_\mathrm{P}^{-1} \\ &= k_\mathrm{P} \circ R_{n-m} \circ k_\mathrm{P}^{-1} \end{aligned}$$

is a member of $\mathcal{Q}_3[k_\mathrm{P}]$, and we can apply the techniques of the previous two sections to find k_P. Our only worry is that $n-m$ be not 13. Similarly,

$$q_2 \circ q_1^{-1} = k_\mathrm{C} \circ R_{n-m} \circ k_\mathrm{C}^{-1}$$

is a member of $\mathcal{Q}_3[k_\mathrm{C}]$, allowing us to find k_C.

Let us look back at our example Q4 key table:

	plaintext letters
	ABCDEFGHIJKLMNOPQRSTUVWXYZ
k_1	OWRXUTMYJZSBPKACEVNFQLIGDH
k_2	SFALCRYIWGHUTXBDJEZKPMNOVQ
k_3	KRNUOIDVTWXGYBZSPQJAMCEFHL
k_4	GJTKBPLMENOAQFRUVDIWHXYZCS
k_5	YCSEPOWFULIQGVHTBAXDZJKMRN
k_6	RYVZWDOSMPAJCNEFLXQIUGHTKB

The shift key is recognizable and appears in the column under plaintext F. This tells us that k_P begins with the letter F. We now pick one of these permutations and compose the others with its inverse on the left:

		order
$k_1^{-1} \circ k_1$	ABCDEFGHIJKLMNOPQRSTUVWXYZ	1
$k_1^{-1} \circ k_2$	KTOVPCHWBXZEFDLYIQJNMGSARU	26
$k_1^{-1} \circ k_3$	NCSEAWYRFBDXHLJKMUIOGPQTZV	26
$k_1^{-1} \circ k_4$	XIFNLMVGQSAOUTCERYWBZDHJPK	26
$k_1^{-1} \circ k_5$	HPKQMABTEVWUXRZFLODYJINGCS	26
$k_1^{-1} \circ k_6$	CHRJBYAKGMOIPSQTVDUWEXZFNL	13

The shift key no longer appears, but we do see it after it has undergone a monoalphabetic substitution using key k_1^{-1}:

$$S\,(k_1^{-1}, \mathtt{TRIPOD}) = \mathtt{FCWMAY}$$

We are lucky to have some order-26 permutations to use for keyword recovery. From $k_1^{-1} \circ k_2$ we obtain the base key

$$k_P = \mathtt{FLYINGSAUCERBDHJKMOPQTVWXZ}$$

as we knew we should. Next we work on k_C by composing with k_1^{-1} on the right.

		order
$k_1 \circ k_1^{-1}$	ABCDEFGHIJKLMNOPQRSTUVWXYZ	1
$k_2 \circ k_1^{-1}$	BUDVJKOQNWXMYZSTPAHRCEFLIG	26
$k_3 \circ k_1^{-1}$	ZGSHPAFLETBCDJKYMNXIOQRUVW	26
$k_4 \circ k_1^{-1}$	RAUCVWZSYEFXLIGQHTOPBDJKMN	26
$k_5 \circ k_1^{-1}$	HQTRBDMNKUVJWXYGZSIOPACEFL	26
$k_6 \circ k_1^{-1}$	EJFKLITBHMNGOQRCUVADWXYZSP	13

The shift key has reappeared, but in the column indicating its own first letter; this will not help us resolve k_C. Using the techniques for keyword recovery in the Q3, $k_2 \circ k_1^{-1}$ gives us the other base key:

$$k_C = \mathtt{SPACEFLIGHTBDJKMNOQRUVWXYZ}$$

Having both base keys, we now know this Q4 completely.

Conclusions

A well-written article has no need for additional comments, and a well-read article does not need a summary. Nevertheless, an article without a concluding section does not get published. So here we are.

We looked at the group theory of the alphabetic permutations used by classical substitution ciphers. Surprisingly, we found that the Beaufort and Porta ciphers are members of the quagmire family. Our most significant result is the observation that a quagmire 3 is isomorphic to the Vigenère, which in turn has the same structure as $\mathbb{Z}_{26}$. This allowed us to develop a new way to expand our knowledge of the keys in attacks on ciphertexts that are based on cribs, and to understand more deeply the process of recovering keywords.

As classical ciphers are little more than recreational in the modern era, the application of group theory to them is for the most part an intellectual exercise. Modern cryptography, especially public-key cryptography, involves group theory intimately. Extending these ideas to the classical ciphers is an interesting field that has so far been overlooked.

References

[1] Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; archive.org/details/cryptanalysis00gain.

[2] American Cryptogram Association, "The ACA and You," www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf; 2005 version: web.archive.org/web/*/http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf; 2016 version: web.archive.org/web/*/http://cryptogram.org/docs/acayou16.pdf; the pages about ciphers are linked from this page: www.cryptogram.org/resource-area/cipher-types.

[3] Saunders MacLane and Garrett Birkhoff, *Algebra*, 3rd edition, New York: AMS/Chelsea, 1988.

[4] Thomas Kaeding; "Quagmire ciphers, group theory, and information: Key amplification in crib-based attacks," Cryptology ePrint Archive, report 2022/1382; "Quagmire ciphers and group theory: Recovering keywords from the key table," Cryptology ePrint Archive, report 2022/1475; "Quagmire ciphers and group theory: What is a Beaufort cipher?", Cryptology ePrint Archive, report 2022/1488; "Quagmire ciphers and group theory: What is a Porta cipher?", Cryptology ePrint Archive, report 2022/1677.

[5] Abraham Sinkov, *Elementary Cryptanalysis: A Mathematical Approach*, 2nd edition, revised by Todd Feil, published by Mathematical Association of America, 2009, www.jstor.org/stable/10.4169/j.ctt19b9krf.

[6] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, 2nd edition, New York: Springer, 2014.

[7] Blaise de Vigenère, *Traicté des chiffres ou secrètes manières d'escrire*, Paris: Abel l'Angelier, 1586, HDL: 2027/ien.35552000251008, http://gallica.bnf.fr/ark:/12148/bpt6k1040608n, http://gallica.bnf.fr/ark:/12148/bpt6k94009991.

[8] R. Morelli and R. Walde, Evolving keys for periodic polyalphabetic ciphers, Proceedings of the Nineteenth International Florida Artificial Intelligence Research Society Conference, 445-450, http://www.aaai.org/Papers/FLAIRS/2006/Flairs06-087.pdf, last modified July 7, 2006.

[9] Thomas Kaeding, Slippery hill-climbing technique for ciphertext-only cryptanalysis of periodic polyalphabetic substitution ciphers, *Cryptologia* 44:3 (2020) 205-222, DOI: 10.1080/01611194.2019.1655504.

[10] Giovan Battista Bellaso, *La Cifra del Sig. Giouan Battista Belaso* [sic], 1553.

[11] Paolo Bonavoglia, Bellaso's 1552 cipher recovered in Venice, *Cryptologia* 43:6 (2019) 459-465, DOI: 10.1080/01611194.2019.1596181

[12] J. Rives Childs; German Military Ciphers from February to November, 1918; 1918; https://www.nsa.gov/Portals/75/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_268/41784789082381.pdf.

[13] Hans van der Meer, An old challenge, 2010, https://staff.fnwi.uva.nl/h.vandermeer/pubs/fuergod.pdf.

[14] C. E. Shannon, A mathematical theory of communication, Bell System Technical Journal 27:3 (1948) 379-423.

[15] Kasiski, F. W. 1863. Die Geheimschriften und die Dechiffrir-Kunst. Berlin: E. S. Mittler und Sohn.

[16] W. F. Friedman, The index of coincidence and its application in cryptography, Riverbank Laboratories Department of Ciphers publication 22, Geneva, Illinois, 1920.

[17] W. F. Friedman and L. D. Callimahos, Military cryptanalytics, Part I, Volume 2, Aegean Park Press, 1956, reprinted 1985.

[18] M. Mountjoy, The bar statistics, NSA Technical Journal VII (2, 4), 1963.

[19] Thomas H. Barr and Andrew J. Simoson, "Twisting the Keyword Length from a Vigenère Cipher," *Cryptologia* 39:4 (2015) 335-341, DOI: 10.1080/01611194.2014.988365.

[20] Auguste Kerckhoffs; "La cryptographie militaire," *Journal des sciences militaires* IX (1883) 5-39 and 161-191, www.petitcolas.net/kerckhoffs/crypto_militaire_1_b.pdf, www.petitcolas.net/kerckhoffs/crypto_militaire_2.pdf; *La Cryptographie Militaire ou des Chiffres Usités en Temps de Guerre*, Paris: Librairie Militaire de L. Baudoin et Co., 1883.

[21] William F. Friedman, The Principles of Indirect Symmetry of Position in Secondary Alphabets and Their Application in the Solution of Polyalphabetic Substitution Ciphers, Washington D.C.: U.S. Government Printing Office, 1935, www.nsa.gov/Portals/70/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_226/41760669079979.pdf.