Quagmire ciphers, group theory, and information:
Key amplification in crib-based attacks

Thomas Kaeding
uvcclxvggl@cebgbaznvy.pbz (to combat spam, my email has been ROT13'ed)
October, 2022

We demonstrate how to apply some ideas from group theory to quagmire ciphers. Techniques are shown for amplifying one's knowledge of the keys. This is useful when breaking a ciphertext with a crib. The basic idea is that only a small amount of information goes into building a key table for a quagmire cipher, so we should only need that much information to reconstruct it.

Introduction

The quagmire ciphers [1, 2] (also known as type 1, 2, 3, and 4 periodic polyalphabetic substitution ciphers) are generalizations of the Vigenère cipher [3] in which the plaintext alphabet is deranged, or the ciphertext alphabet which slides against it is deranged, or both. Another way of thinking about them is as a table of twenty-six monoalphabetic substitution keys. A subset of them is chosen and applied in repeated sequence to the letters of the plaintext to create the ciphertext.

Our convention is to call the table of repeated alphabet keys the "key table" for the cipher, and the full list of all possible alphabet keys for a given keyword its "tableau". Each row of the key table or of the tableau is an alphabet key for a monoalphabetic substitution and contains each of the twenty-six letters; i.e., it is a permutation of them. For the quagmire ciphers it is also the case that each column of the tableau contains each of the twenty-six letters. This ensures that for any ciphertext character, there exists a key that can decrypt it.

All monoalphabetic substitution keys are members of the permutation group on twenty-six objects. If you don't know what that means, do not fret: to learn the techniques described in this paper does not require that you understand why they work. On the other hand, if you are interested in learning about groups and their properties, there are plenty of good textbooks on abstract algebra, such as that one by those two guys [4].

The main goal of this paper is to show how partial knowledge of the key table of a cipher can be amplified to nearly complete knowledge of it. The idea is that there is a lot of redundancy in quagmire key tables, but only so much information in the keys. That information is smeared out over the key table. When we have a sparse knowledge of the key table, namely few characters in it, we can use the structure of the cipher and the redundancy built into it to fill in more characters. The techniques for doing so will rely more and more heavily on group theory as we advance from the Vigenère cipher to the quagmire 4.

We are going to start off slow, with the Vigenère cipher, and work our way to the more interesting stuff. If you know the quagmire 1 and 2 ciphers very well, then the tricks we use on those two may seem familiar. But please bear with us; they lay the foundation for what follows. The good stuff starts when we get to the quagmire 3.

Permutation group

A key for a monoalphabetic substitution is simply a permutation, or rearrangement, of the alphabet. All of our examples will use the same keywords. Using OPHELIA, we construct this key:

```
OPHELIABCDFGJKMNQRSTUVWXYZ
```

What this means is that a substitution cipher using this key will change A to O, B to P, etc., as we can tabulate so:

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

We need a way to combine two keys, when one acts on a plaintext and the other then acts on the first one's ciphertext. If $S\ (k,\ t)$ denotes a substitution cipher with key k acting on a text, then the combination of two keys can be found by taking $S\ (k_1,\ k_2)$, i.e., by treating one as a text. In this way we define a binary operation on key, which we will call "multiplication":

$$k_1 \circ k_2 \ = \ S\ (k_1,\ k_2)$$

Since this merely permutes a permutation of the alphabet, the result still contains all twenty-six letters and is therefore also a permutation, i.e., a key. That means that the set of keys is closed under this operation. It also turns out that the operation is associative:

$$(k_1 \circ k_2) \circ k_3 \ = \ k_1 \circ (k_2 \circ k_3)$$

So we can drop parentheses everywhere. However, be aware that in general, the operation is not commutative. This means that the order in which we multiply them matters; we can't switch them around.

Let's do an example of multiplication. Consider these two keys:

k_1 = HAMLETBCDFGIJKNOPQRSUVWXYZ
k_2 = OPHELIABCDFGJKMNQRSTUVWXYZ

The first takes the unscrambled alphabet into 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
H A M L E T B C D F G I J K N O P Q R S U V W X Y Z
```

The second takes the first key and encrypts it.

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

So the H becomes B, A becomes O, M becomes J, etc. The product is

$k_2 \circ k_1$ = BOJGLTPHEIACDFKMNQRSUVWXYZ

We will often need to be able to multiply keys when we do not have complete knowledge of their entries. In that case, our lack of knowledge will propagate. Let's reconsider our example, but leave out some letters:

k_1 = HAM·ETBCD···JKN·PQR··VWXYZ
k_2 = OPHEL··BCD·G·KMNQ·STUVW·YZ

When we take the product, H still becomes B, and A becomes O, but M maps to an unknown letter. The next letter in k_1 is also unknown, so it remains so. Then E becomes L, etc. The product is

$k_2 \circ k_1$ = BO··LTPHE···D·K·NQ···VW·YZ

The unmixed alphabet serves as the identity element of the group, so we will often denote it as e. The identity element has the property that when it is multiplied by any other key, the result is unchanged:

$$e \circ k = k \circ e = k$$

If we can scramble the alphabet, then we can unscramble it. In other words, every permutation (key) has an inverse. To find an inverse, we list the key under the unscrambled alphabet, then rearrange the columns until the lower row is unscrambled. The top row is then the inverse key. For our example,

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

becomes

G H I J D K L C F M N E O P A B 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

The inverse, which we denote as k^{-1}, is

GHIJDKLCFMNEOPABQRSTUVWXYZ

When we multiply a key by its inverse, from either side, we get the unscrambled alphabet e:

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

Again, we will often need to work with keys with missing information. So we need to know how to invert a key with missing letters. Again, our ignorance propagates. For example, suppose we want to invert this key:

OPHEL··BCD·G·KMNQ·STUVW·YZ

Line it up with the unscrambled 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
O P H E L · · B C D · G · K M N Q · S T U V W · Y Z
```

Rearrange so that letters in the lower row are in the positions they would have in the unscrambled alphabet:

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

The letters in the top row that are above a gap become unknown letters in the inverse key, which we have found to be

```
·HIJD·LC··NEOPABQ·STUVW·YZ
```

Integers modulo 26

It will soon become obvious why we should want to understand the integers modulo 26, Z_{26}. For those of you who do not know the word “modulo,” we will explain. We take the set of numbers {0, 1, ..., 25}, and whenever we do arithmetic on them, if the result is outside that range, we add or subtract enough 26’s to bring us back inside. The number 26 is called the “modulus.” The only arithmetic we are going to be doing is addition, and maybe subtraction, so do not worry.

Addition is defined in the obvious way. We add two numbers as usual, then subtract 26 if the answer is greater or equal to 26. So $11 + 23 = 34 \rightarrow 10$. The additive inverse of number n is found as $26 - n$, and the identity element is 0. As you can guess, my next statement is that Z_{26} with addition is a group.

Now let us talk about the order of its elements. The order of a group element is the smallest number of that element that need to be added together to get the identity. Sometimes the answer is obvious, like $13 + 13 = 26 \rightarrow 0$, so the order of 13 is 2. But other times it is not so obvious, like $4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 = 52 \rightarrow 0$, so the order of 4 is 13. Here is a table of all of the elements of Z_{26} and their orders:

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

Notice that some elements have order 26, which is the largest that it can be. Such an element is called a "generator," since by adding it successively to itself, the sum runs through the entire group. In other words, we can obtain every element of the group by finding multiples of one generator. Also, notice that the elements that are generators share no factors with 26; the greatest common denominator in those cases is gcd (n, 16) = 0. We say that these element are coprime with 26.

You might also notice that there are many generators. And there are many with order 13. It is possible to shuffle them around and still keep the same group structure. A mapping that takes one set with a binary operation to another set with its own binary operation in such a way that the structure is preserved is called an isomorphism. Preserving the structure means that the mapping φ has this property:

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

where the little black square represents whatever binary operation is appropriate. When the two sets in question are actually the same set, then the mapping is called an automorphism. Here is one automorphism of Z_{26}, in which we simply multiplied every element by 5 (which is a generator):

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

Notice that 0 maps to 0 and 13 maps to 13; an element must map to one with the same order. Knowing that there are many ways to map into Z_{26} can be useful near the end of this paper.

Vigenère cipher

If you are reading this, and I know you are, then you are already familiar with periodic polyalphabetic substitution ciphers. However, in anticipation of more interesting things, we begin slowly and simply with the Vigenère cipher. The key of a Vigenère with period *m* contains *m* letters. We can therefore say that the shift key has *m* letters of information in it. This shift key is not to be confused with alphabet keys, which are the permutations. At the risk of being pedantic and even ridiculous (please bear with me), we can say that the informational content (thinking along the lines of [5]) of the key is

$$I = m \cdot \log_{26}(26) = m$$

characters. The 26 inside the logarithm reflects the fact that there are twenty-six choices for each letter of the key. We need at least this much information to break a Vigenère cipher. From this we conclude that we can use a crib of length *m* to reconstruct the key table for a given master key.

To help us in reconstructing a key table, we recall that each of its rows is a rotation of the unmixed alphabet. If we denote rotation by *n* steps as $R_n(x)$, Then each alphabet key can be thought of as $R_n(e)$, for some *n* and where *e* denotes the unmixed alphabet.

At further risk of ridicule, let us present an example of a crib-based attack. We will work the example in what may appear to be overly drawn out and silly, but it will help get into a way of thinking that will help with the quagmire ciphers. Here are the first fifty characters of Hamlet’s soliloquy, encrypted with period of six:

AONPSK UOFESU LTTLXB ZTTPUN LSFTSG DHQELX YTUDRH ILQCMG AH

We need a crib that provides enough information to reconstruct the key table, and so we need six characters. Take the first six letters of the plaintext:

tobeor

With this crib and the first six letters of the ciphertext, we find this much of the key table:

	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						
k_2															O											
k_3		N																								
k_4					P																					
k_5															S											
k_6																		K								

(Here and throughout this paper we assume that the period is known. We can usually find it from the Kasiski method [6, 7], index of coincidence [8, 9, 10] by trying various periods until a suitable one is found [11]. Another option is the twist method [12].) The plaintext alphabet is along the top of the table, and characters of the individual keys appear in the bulk of the table. We see an A under the t in the first key to indicate that t is encrypted to A by k_1. This also indicates that the first key is $R_7(e)$, since we are taking leftward rotation to be the positive direction. Now, this may seem especially ridiculous, but let us apply the inverse rotation on the first row of the table to get

$R_7^{-1}(k_1)$ = A·························

Here, · denotes an heretofore unknown character. Since the unrotated key must be the straight alphabet, we can fill in the missing letters and write

$R_7^{-1}(k_1)$ = ABCDEFGHIJKLMNOPQRSTUVWXYZ

Rotate back to get:

$k_1 = R_7(R_7^{-1}(k_1))$ = HIJKLMNOPQRSTUVWXYZABCDEFG

Following the same procedure for the remaining five rows of the table, we obtain the full table:

	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	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
k_2	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_3	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
k_4	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_5	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_6	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

We say that we have “amplified” our knowledge of the key table. We realize this technique seems so trivially obvious, and you do it without even thinking about it, but things will get more interesting. Trust us.

Let’s pause for a moment and consider the full tableau for the Vigenère cipher:

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	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	Z

We have written the unaltered plaintext alphabet across the top. On the left are letters from which the shift key is made. For each shift we have a rotated alphabet. It should be clear that the possible monoalphabetic keys for the Vigenère are R_0 (e), R_1 (e), ..., R_{25} (e), where as usual e denotes the unmixed alphabet. For convenience, we will write R_0, R_1, ..., R_{25}. Of course, $R_0 = e$.Notice that each letter occurs exactly once in each column. This is true also for the quagmire ciphers, and we will refer to this as the "column property."

Now, the action of the binary operation on two alphabet keys from the Vigenère cipher is another member of the set of Vigenère alphabet keys. This should be obvious, since each key is a rotation R_n of the unmixed alphabet, and when two rotations are combined, the result is to add their numbers of steps:

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

Of course, we must evaluate the sum $m + n$ modulo 26. Because addition is commutative, so is the composition of rotations:

$$R_m \circ R_n = R_n \circ R_m$$

So what we have is a commutative (most call it abelian) subgroup of the group of all alphabet keys. Furthermore, this subgroup is isomorphic to Z_{26} with addition. The most natural isomorphism is

$$R_n \rightarrow n$$

and the group structure is preserved because

$$R_m \circ R_n \rightarrow m + n$$

These results may seem trivial, but we will see similar structure in the quagmire 3 cipher, where things are less obvious.

Quagmire 2

Wait, what? Did we skip something? No, we are going to do the quagmire 2 before the quagmire 1 because it is much easier.

The quagmire 2 cipher (Q2) uses an unmixed plaintext alphabet sliding against a mixed ciphertext alphabet [1, 2]. Alternatively, we can build a tableau from the keyword used to mix the ciphertext alphabet, and select those rows that correspond to letters in the shift key. The key generated from the keyword we will call the "base key." For example, using the keyword `OPHELIA`, our base key is

$$k_{\text{base}} = \texttt{OPHELIABCDFGJKMNQRSTUVWXYZ}$$

From it, the tableau generated is

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

Notice that each row is a rotation of the base key, and that we have the “column property.”

The quagmire 2 cipher can be factored into a Vigenère cipher followed by a monoalphabetic substitution [13, 14]:

$$Q_2\ (k_{\mathrm{v}}, k_{\mathrm{base}}, t) \ = \ S\ (k_{\mathrm{base}}, V\ (k_{\mathrm{v}}', t))$$

Here the alphabet key is the base key, but the shift key k_{v}' here is not the same as the keyword k_{v} for the Q2 cipher, but rather the m characters given by

$$k_{\mathrm{v}}' \ = \ S^{-1}\ (k_{\mathrm{base}}, k_{\mathrm{v}})$$

because it has passed through the substitution cipher. This factorization should be obvious from looking at the tableau: clearly, shifts are taking place, followed by substitutions. We can therefore write any key from the table as

$$k_n \ = \ k_{\mathrm{base}} \circ R_n$$

If we multiply two Q2 keys we get

$$k_m \circ k_n \; = \; k_{\text{base}} \circ R_m \circ \; k_{\text{base}} \circ R_n$$

This is not of the same form as the previous relation. So immediately we see that the set of Q2 keys is not closed under our binary operation. We do not have a group. Instead, what we have is a coset of the Vigenère subgroup. We call it a left coset because the constant (k_{base}) is multiplied on the left. The relation $k_n = k_{\text{base}} \circ R_n$ provides a mapping from the Vigenère group into the Q2 coset; however, it is not an isomorphism, and we have lost the group structure. We don't even have commutation any more.

How much information is contained in the keys? The shift key contains m independently chosen characters, providing m characters' worth of information. The first letter of the base key provides one character's information. However, there remain only twenty-five options for the second letter; so the second carries less information. By the time we reach the end, there is only one choice for the final letter, so it provides no information. The total is

$$I \; = \; m \; + \; \log_{26} 26 \; + \log_{26} 25 \; + \; \log_{26} 24 \; + \; ... \; + \log_{26} 1 \; = \; m + \log_{26} 26! \; = \; m \; + \; 18.8$$

This means that theoretically we need m+19 known entries in the key table in order to fully reconstruct the table when we are breaking a ciphertext. Practically, however, the characters that we find may likely have overlapping contributions to the information, so more than m+19 are needed. Furthermore, due to the redundancy of language, we need an even longer crib. The same equation and same arguments hold for the quagmire 1, 2, and 3 ciphers.

The procedure for key amplification is simple: Since all keys are rotations of one key (the base key), we rotate our incomplete keys until they are aligned. Then we can collapse them into one key by combining all the knowledge we have. Then unrotate each and put them back into the key table.

Let us work through an example. Take Hamlet's soliloquy once more, and encrypt it with a Q2 cipher using shift key `HAMLET` and base key `OPHELIABCDFGJKMNQRSTUVWXYZ`. The full ciphertext is

```
VUNCRFNUBXRUAZVLWPUZVCTKAYBJRAYKSXFXTZWWQBERSVGAVKSQGAIZHWX
YBFIXFXURWRDGHTRLUFQHASCBWZILDXQOADRFVOPCRFVUBLKXHXOWEZHMPW
WTUFMSCJTUCIMXUAPBLRQVESVPNJSRAJDFOXRWFFBSVLAFERRIQXSLQWELM
WMXAVBSVTOHSCQWVKSGBTTZMAFXHTRXFXVKHYVTNDPLWKTAZWFBLQAXFTVG
ZCVOFYVCGFVUBJVTLUPWXIMABJRAIFDSXJKLBSLXYMAGAJQDWCWBURSCSJQ
YZCBCRFIAFTNCSXRWTFMQERVKSVBGVKSVXUBUIJQJDABWMXAVHDAXHZVOFT
VDICEIUSMHIBMFFGBAYFVLYXUKCDCLADHDCJDMAQRFVAZARPKSCWWZFPSYV
CHOACWOAXSWWOAXSWSXLZBGEJMAYCVVHRMQGJOUTWRLQTUNGYAGHVZOQHHY
MWEFMVWOAHVJSGHTRWIBTTASCJFSSXFBRVICVGQXAOUBNJBGBCTUCBNTNYQ
SQJWSSNPJDFELQZUUTBGGRXWEALQPSXFXKAFWAXKAJXFXFTASMXNCSSCBBG
WABTNDBGBGROIRVJDABTEJFFPXNXTMBSCJDOPORFVKJXEEAYFGBADFVJNGA
RTQGZDZVJVDWMSXXGMAYCZPVKMIEFABHBKPNHVSZBWRRDEFIFZWLXHXBSDF
WTBLQWUHSLWKNDSVENAAIHMPBFNYWJDABXFXIXSLABBYHQBJDMPFEYVFIBB
TVKBGBKNDWWIBXFICAVQOPXURBXHQZOQYSIRKTTPSWFHPSNMXTXSXXFNYEY
HSKFAXFXYMZNEAISMMBGWYILWOAXNCEFVKHWBPKRAOBOHPSXFTNGZHWBQZV
CUGVKMXZXJTHOQBVUTXFKUCHRVVFFPABWQZVQEEACHOEFIYHDXGHRZLQWVK
CWWOATMXGMAKCCRYTFASMKVMHRGGUMQMMPADHCUNFZVXFXRAZCITUZHDWOQ
```

```
OUGWTNDSRWXTVIJVXUUTFUXHZEJWOHTRQRIATBOGJDZVJVFAJMVAJDFWVIK
TXSRWGVOIRENTLMRALQYSXFXNAOCRYHCBJRA
```

As our crib, take the first 50 characters of the plaintext:

```
VUNCRF NUBXRU AZVLWP UZVCTK AYBJRA YKSXFX TZWWQB ERSVGA VK
tobeor nottob ethati sthequ estion whethe rtisno blerin th
```

Comparing the plaintext and ciphertext gives us this much information about the key table:

	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 |		E			A									N				T	U	V			Y			
k_2 |								K				R			U				Y	Z						
k_3 |		N			S			V	W											B						
k_4 |	L				C				J									V	W	X						
k_5 |								F	G					Q	R		T			W						
k_6 |		U			X				P					A	B			F			K					

If we try to finish the decryption with this much information about the key, this is what we get:

```
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHE.IN.T.S.
....THESLI......A.R.....O.T.A.E....ORT..EORTOTA.E...S.....S
T.S.....RO...ES..........IN.E......TO...T...E...O...EAN.B..
S.EE.T.....EEN.THE...RT..HE...THETH....N..ATUR..SHO...TH.T.
.E...SHEIRTOTI...O.S....TION........T..EW.......IETOSLEE...
S.E......H.N.ETO.R.....THER..THER.B.O.IN...TS.EE....E.TH.H.
T..E..S....O.....NW.HA.ESH....E.........ORT...OI...ST...E..
....ET.E.EST.E.ES.E.TT......E...L..I..O.SO.....I.E..R......
..B..RT.E.HI.....S.OR.......ETHO...E.......ON.T...RO....NS.
.N...E......AN.SO..I...I.....ETHE...S.E...THE.....EN.E..O..
I...N.T...........T......T.ER.T.......ORTH.T..ES...N..HI..E
L..I..THI....ET.....E.ITH...RE....IN.H..O.L...R...S.E..T..R
..TAN.S.EATUN.ER..E....I..B.T...TTHE..EA.O.S..........T....
.THT..UN.IS.O...E.....T.........SE.OUR...TR..E..ER.ET.RNS..
.....THEW....N.......S.AT.E.BE.RTH.S.I.L......ETH.N...TO.TH
E..TH.T.E....NOTO.THUS...........TH...E....R.S.....L.AN.TH
.ST.E..TI.EH.EO.R....UT...I.S....IE..E...THTHE...E..ST..T..
...T.N.E.TER..I.ESO...E.T.IT.....O.E.T.I..THI.RE..R....IR.U
R.E.T.T.....R......SETHEN..EO...TION
```

To begin the amplification, take the keys and rotate them until they are aligned. We do this by rotating until we see that each shares a character in the same column as another. This works uniquely because of the “column property” (and hopefully we have found enough characters in the table).

```
TUV··Y····E··A········N···
·U···YZ·············K···R·
··VW··········B·······N··S
··VWX······L···C···J······
T··W·············FG····QR·
·U··X···P····AB··F··K·····
```

The numbers of step in the rotations (taking leftward to be positive) are 17, 13, 6, 15, 16, 0. We must remember them, since we need them later. Now collapse them all into one key:

```
TUVWXYZ·P·EL·ABC·FGJK·NQRS
```

Make six copies and unrotate them (remember those numbers?):

	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		E	L		A	B	C		F	G	J	K		N	Q	R	S	T	U	V	W	X	Y	Z		P
k_2	A	B	C		F	G	J	K		N	Q	R	S	T	U	V	W	X	Y	Z		P		E	L	
k_3		N	Q	R	S	T	U	V	W	X	Y	Z		P		E	L		A	B	C		F	G	J	K
k_4	L		A	B	C		F	G	J	K		N	Q	R	S	T	U	V	W	X	Y	Z		P		E
k_5	E	L		A	B	C		F	G	J	K		N	Q	R	S	T	U	V	W	X	Y	Z		P	
k_6	T	U	V	W	X	Y	Z		P		E	L		A	B	C		F	G	J	K		N	Q	R	S

That is quite an improvement. Here is what we get if we decrypt with it:

```
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHEMIN.T.SU
FFE.THESLIN.S.NDARRO.SOFOUT.A.EO.S.ORT.NEORTOTAKE.R.SAG..NS
TASE.OFTROU..ESANDBYOPPOSINGENDT.E.TODIETOSLEEPNO.OREANDBY.
S.EEPTOSA..EENDTHEHEART.CHE.NDTHETH.USAN.NATURALSHOCKSTHAT.
LES.ISHEIRTOTISACONSU..ATION.E.OUTLYTOBEW.SHDTO.IETOSLEEPTO
SLEEPPE.CHANCETODRE.MAYTHERESTHERUBFO.INT.ATS.EEP..DE.TH.HA
T..EA.SM...O.EWHENWEHAVESHU.FLE...FT..SMORTALCOILMUSTGIVEUS
P..SET.EREST.ERESPECTTHAT.AKESC.L.MIT.OFSOLONGLIFE..RW.O..U
.DBE.RT.E.HIPS.NDS.ORNSOFTIMETHOPP.ESSORS.RONGTHEPROUDMANSC
ONTUMELYT.EPANGSOFDISPRIZDLOVETHELAWSDELAYTHEINSO.ENCEOFOF.
ICEAN.THESP..NST.ATPATIENTMER.TOFT..N.ORTHYTAKESWHEN.EHIMSE
LFMIG.THIS.U.ETUS.AKEWITH..AREB.DKIN.HOWOULD.AR.ELSBE.RTO.R
UNTANDS.EATUN.ERAWEA...IFEBUTT.ATTHE.READOFS.MET..NGAFTE.DE
ATHTHEUN.IS.OVE.EDCO.NTRYFR.MW.OSE.OURNNOTR.VEL.ERRETURNSPU
.ZLESTHEW.LLAN.M..ESUS.AT.ERBEARTH.SEILLS.E..VETHAN.L.TOOTH
ERSTH.TWEKN..NOTOFTHUSC.NSCIENCEDOTHMAKEC..AR.S..US.LLANDTH
UST.EN.TI.EHUEOFRESO.UT..NISS.C..IE..ERWITHTHEPALE.AST..T.O
.GHTAN.ENTERP.ISESOFGRE.TPIT..NDMO.ENT.IT.THISREG.RDT.EIR.U
RRENTST..NAWRY.NDLOSETHENA.EOF.CTION
```

We are sure that you, dear reader, were already familiar with this technique. But now let’s turn the the quagmire 1 (Q1) and see a slightly more complicated procedure.

Quagmire 1

In the quagmire 1 cipher (Q1), an unmixed ciphertext alphabet is slid along a deranged plaintext alphabet [1, 2]. A keyword is used to derange the plaintext alphabet, which we will call the base key k_{base}. From this it should be clear that the tableau (above which is an unmixed plaintext alphabet) contains the inverses of shifted versions of the base key, and that the cipher can be factored into a monoalphabetic substitution followed by a Vigenère cipher [13, 14]. The substitution is the inverse of the base key:

$$Q_1 (k_{\mathrm{base}}, k_{\mathrm{v}}, t) \;=\; V (k_{\mathrm{v}}, S^{-1} (k_{\mathrm{a}}, t))$$

Here k_{v} denotes the shift key, containing m characters, and k_{a} is a rotation of k_{base} so that A is in the first position. In terms of keys, what we have are keys of the form

$$k_n \;=\; R_n \circ\; k_{\mathrm{base}}{}^{-1}$$

We see that we have a coset of the Vigenère group, but a different kind, because the multiplier is on the right instead of the left. We call this set a right coset. But let’s invert it. Since when we invert a product of permutations, we get inverses of them in reverse order, the inverse of the above is

$$k_n{}^{-1} \;=\; (R_n \circ\; k_{\mathrm{base}}{}^{-1})^{-1} \;=\; k_{\mathrm{base}} \circ R_{-n}$$

Now we have a coset of the kind we saw in the case of Q1, and we can reuse the technique we have for amplifying the key table.

Let us see for ourselves with an example. Consider our favorite base key:

$$k_{\mathrm{base}} \;=\; \texttt{OPHELIABCDFGJKMNQRSTUVWXYZ}$$

From it we build this tableau:

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

The inverses are:

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

As you can see, we have the same pattern we saw in the quagmire 1, i.e., rotated versions of the base key. They may be in a different order, but that is no matter.

The strategy for amplifying the key table from limited knowledge of its entries is to first invert each row, and then, since we know that these inverses are rotated versions of one another, we look for letters in common so that they can be rotated into alignment. Then, some missing letters from one may be borrowed from another. We reconstruct as much of the base key as possible. The base key is unrotated appropriately for each row of the table, and inverses are taken.

Let us work through an example to show how this strategy helps with a crib-based attack. Take once again Hamlet’s soliloquy, but this time encrypted with a quagmire 1 cipher, again with period six. Here is the full ciphertext:

```
UUNIYEQUZYYUENILRSTNIIOHEMZKYCXWJYAQSNLXNNIYJWDCUWJTDCKNGXS
XLXXYAQTYLUJFHJPLPEBQYFINVNXLJQBOYPYEUOVIYEUUZLLQHLUXEYHZVX
RTTXMFIGSUAMCQTAVOFLBVHFQSQFJUHGDXUYYWGXZFQREXHUYBBLJLNWISM
XCQEVZFQTZQJINWUWJHBTSNMNAQHJPYAQUWGZQTQDVLRHSAKXANJHYYATUE
KIQPGMIIDEUUZKQTJUVXSBPAZKYCKXBFSGFSZFFQXZYHHGBDLIRNTYJIZGB
MKIBOCXXNATQCJYYWSXMTELUWJWBFUWJWSULUXKNGDAZXCQEVGPHQHNIBAT
UDXIEBTIMDGNPXCHBCXXILTQTWAPIREDGPIGDZYTYEUAKNYSFIAXRYGPJZQ
```

```
OHOYIRPELJXRPELJXZQJNZHEGPATIQVHYMTDGZUQXYRBJRJDXEEGWUPBQGZ
CWIXMWRPEQIKZFHJPXGNSJYFIGGIJYANCVXIQFBLYBPNQFZHBOSUAOMTQMO
FNGVIJJWGDXHLNYTUQODFCLLEHRBPJYAQFACXHQFAEYAQGJYFCQQCJFINLE
LNBTQDZHBFCOXUQGDAZGEGGXVYMQSZZFIGDOVBYEUWEYEAEMCHBCDXIKMFE
YQTDYDNIKQDVZJYSFPATIUSUWMMEEEBGOLSQQIFUNVYPPEEKXKXFQHLZFJE
VJZLNWTQJLRHQDJWEJEAXDCSLXNZRGDAZYAQKLJLHNLMGTBGDZVQEXUXXOB
TUWZHBHQDLXGNWXXIHVBOVYPLLLGTUPBMJMYHSJVFREHPJJCQSLJYSEQMHZ
XMFXYYAQXZKJECKIMSBFVMXLRPELNIEEUWGXBSFYYBBPHPJYATQEKDRNBNI
IPFUWMYUQOJGBNNUUQYAHTCGUQVGXVNBWBNITEAECGBEEKMGPSFHYKLNWUW
AXRPEJMYDIEWAIYXSXYFCHUZGUDFTZOSCSEDGIPJGNIYAQCAKIGTTNGPRPB
ORHRTQDJURQSVXKQQTUQQPQHNHKRPHJPTYBEJZBDGDNIKQEEFMWHGDXLWGH
SLJURFUOXUEJSSMUHRBMJYAQQAUIYXHCZKYC
```

Once again, the first fifty characters of the plaintext will serve as our crib:

```
UUNIYE QUZYYU ENILRS TNIIOH EMZKYC XWJYAQ SNLXNN IYJWDC UW
tobeor nottob ethati sthequ estion whethe rtisno blerin th
```

They give us this knowledge about the key table:

	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		I			E									Q				S	T	U			X			
k_2								W				Y			U				M	N						
k_3		N			J			I	L											Z						
k_4	L				I				K									W	X	Y						
k_5								A	D					N	Y		O			R						
k_6		U			Q				S					C	N			E			H					

Decrypting the full text with this limited knowledge gives this:

```
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHE.IN.T.S.
....THESLI......A.R.....O.T.A.E....ORT..EORTOTA.E...S.....S
T.S.....RO...ES..........IN.E......TO...T...E...O...EAN.B..
S.EE.T.....EEN.THE...RT..HE...THETH....N..ATUR..SHO...TH.T.
.E...SHEIRTOTI...O.S....TION........T..EW.......IETOSLEE...
S.E......H.N.ETO.R.....THER..THER.B.O.IN...TS.EE....E.TH.H.
T..E..S....O.....NW.HA.ESH....E.........ORT...OI...ST...E..
....ET.E.EST.E.ES.E.TT......E...L..I..O.SO.....I.E..R......
..B..RT.E.HI.....S.OR.......ETHO...E.......ON.T...RO....NS.
.N...E......AN.SO..I...I.....ETHE...S.E...THE.....EN.E..O..
I...N.T...........T......T.ER.T.......ORTH.T..ES...N..HI..E
L..I..THI....ET.....E.ITH...RE....IN.H..O.L...R...S.E..T..R
..TAN.S.EATUN.ER..E....I..B.T...TTHE..EA.O.S..........T....
.THT..UN.IS.O...E.....T.........SE.OUR...TR..E..ER.ET.RNS..
.....THEW....N.......S.AT.E.BE.RTH.S.I.L......ETH.N...TO.TH
E..TH.T.E....NOTO.THUS............TH...E....R.S.....L.AN.TH
.ST.E..TI.EH.EO.R....UT...I.S....IE..E...THTHE...E..ST..T..
```

```
...T.N.E.TER..I.ESO...E.T.IT.....O.E.T.I..THI.RE..R....IR.U
R.E.T.T.....R......SETHEN..EO...TION
```

Now let us work on amplifying our knowledge of the key. First, we find the inverses of the six keys:

```
····E···B·······N·RST··W··
············ST······O·H·L·
········HE·I·B···········T
········E·IA··········RST·
H··I·········NQ··T······O·
··N·R··U·····O··E·I·B·····
```

We can align them by rotating as follows, due to the “column property” (which also holds for inverses):

```
··N·RST··W······E···B·····
·····ST······O·H·L········
······T········HE·I·B·····
····RST·········E·IA······
··NQ··T······O·H··I·······
··N·R··U·····O··E·I·B·····
```

The leftward steps are 14, 7, 19, 18, 11, and 0; we must remember these numbers so that later we can undo the rotations. Now we can reconstruct more than half of the base key, or rather, a rotation of it, by including any letter that appears in any of the six:

```
··NQRSTU·W···O·HELIAB·····
```

We can almost see the keyword. At this point, we might fill in by hand some remaining letters; V and XYZ are obvious. If our attack is automated, we may not want to do so. Next we reverse the rotations, using the reconstruction.

```
·O·HELIAB·······NQRSTU·W··
AB·······NQRSTU·W···O·HELI
U·W···O·HELIAB·······NQRST
·W···O·HELIAB·······NQRSTU
HELIAB·······NQRSTU·W···O·
··NQRSTU·W···O·HELIAB·····
```

Finally, we invert each of them and put them back into the key table:

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

As we can see, for any letter that appears in our crib, we are now able to decrypt to that letter, no matter in which slice of the text it appears. As expected, they are the most common letters, which is helpful for breaking the remainder of the cipher. On the other hand, it is a weakness that we only construct those parts of the keys for letters that are found in the crib. Notice that we can read off the shift key from the first column; this is possible because the letter `a` appears in the crib. Here is a decryption of the full text with the amplified key table:

```
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHE.IN.TOSU
..ERTHESLIN.SAN.ARROWSO.OUTRA.EOUS.ORTUNEORTOTA.EAR.SA.AINS
TASEAO.TROUBLESAN.B.O..OSIN.EN.THE.TO.IETOSLEE.NO.OREAN.B.A
SLEE.TOSA.WEEN.THEHEARTA.HEAN.THETHOUSAN.NATURALSHO..STHAT.
LESHISHEIRTOTISA.ONSU..ATION.E.OUTL.TOBEWISH.TO.IETOSLEE.TO
SLEE..ER.HAN.ETO.REA.A.THERESTHERUB.ORINTHATSLEE.O..EATHWHA
T.REA.S.A..O.EWHENWEHA.ESHU..LE.O..THIS.ORTAL.OIL.UST.I.EUS
.AUSETHERESTHERES.E.TTHAT.A.ES.ALA.IT.O.SOLON.LI.E.ORWHOWOU
L.BEARTHEWHI.SAN.S.ORNSO.TI.ETHO..RESSORSWRON.THE.ROU..ANS.
ONTU.EL.THE.AN.SO..IS.RI..LO.ETHELAWS.ELA.THEINSOLEN.EO.O..
I.EAN.THES.URNSTHAT.ATIENT.ERITO.THUNWORTH.TA.ESWHENHEHI.SE
L..I.HTHISQUIETUS.A.EWITHABAREBO..INWHOWOUL..AR.ELSBEARTO.R
UNTAN.SWEATUN.ERAWEAR.LI.EBUTTHATTHE.REA.O.SO.ETHIN.A.TER.E
ATHTHEUN.IS.O.ERE..OUNTR..RO.WHOSEBOURNNOTRA.ELLERRETURNS.U
..LESTHEWILLAN..A.ESUSRATHERBEARTHOSEILLSWEHA.ETHAN.L.TOOTH
ERSTHATWE.NOWNOTO.THUS.ONS.IEN.E.OTH.A.E.OWAR.SO.USALLAN.TH
USTHENATI.EHUEO.RESOLUTIONISSI..LIE.OERWITHTHE.ALE.ASTO.THO
U.HTAN.ENTER.RISESO..REAT.ITHAN..O.ENTWITHTHISRE.AR.THEIR.U
RRENTSTURNAWR.AN.LOSETHENA.EO.A.TION
```

How cool is that, eh?

Quagmire 3

Now for the fun stuff: the quagmire 3 cipher (Q3). In this cipher, both the plaintext alphabet and the ciphertext alphabet that are slid along each other are deranged, and they are deranged in the same way. Like Q1 and Q2, we can factor the quagmire 3. In this case, we find a Vigenère sandwiched between a substitution and its inverse [14]:

$$Q_3\,(k_{\mathrm{base}}, k_{\mathrm{v}}, t) \;=\; S\,(k_{\mathrm{base}}, V\,(k_{\mathrm{v}}', S^{-1}\,(k_{\mathrm{base}}, t)))$$

Here, k_{v} is the shift key for the Q3, but k' needs to be

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

as it was in the Q2 cipher. From this factorization we can see that the keys of the Q3 are related to the rotations in the Vigenère cipher by

$$k \;=\; k_{\mathrm{base}} \circ R_n \circ k_{\mathrm{base}}^{-1}$$

This is both a unitary transformation and an isomorphism, since k_{base} is unitary (it's a permutation) and the group operation is preserved:

$$k_1 \circ k_2 \;=\; (k_{\text{base}} \circ R_m \circ k_{\text{base}}{}^{-1}) \circ \; (k_{\text{base}} \circ R_n \circ k_{\text{base}}{}^{-1}) \;=\; k_{\text{base}} \circ (R_m \circ R_n) \circ k_{\text{base}}{}^{-1}$$

Therefore, the keys in the Q3 tableau form a subgroup that is isomorphic to the Vigenère subgroup, which in turn is isomorphic to Z_{26}. So Q3 is isomorphic to Z_{26}.

This is all good news. First of all, it means that the identity element, which is the unmixed alphabet, is a member of the Q3 tableau. Second, it means that products and powers of Q3 keys are also Q3 keys. This includes their inverses, which are $k^{-1} = k^{25}$. It also means that we have commutivity again, so we can multiply keys from the same tableau in any order.

Our strategy for key amplification will be the following. After acquiring a set of incomplete keys, we will multiply them together in pairs and can take inverses. If the result can be matched to a key already found, then we can merge any new knowledge from the result into the key. That is to say that if we find a key that matches one that we have already seen, we can merge their letters into an improved key. The "column property" that each letter occurs exactly once in each column of the tableau allows us to match keys if they share at least one letter in the same column. If the result of the multiplication or inversion does not match a present key, then we add it to the tableau. Furthermore, if any key has a letter that matches the corresponding plaintext letter, then we know that it is the identity element, and we can immediately fill it in completely. We continue to multiply and invert keys, old and new, until it is no longer possible to gain any more knowledge about the tableau. Finally, we select the keys that belong in the key table (i.e., those that can be matched with the original incomplete keys) and use them to improve our decryption.

Let us look at an example. We return to our favorite base key:

$$k_{\text{base}} = \texttt{OPHELIABCDFGJKMNQRSTUVWXYZ}$$

It generates this tableau for the Q3 cipher:

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

Notice that the tableau is symmetric, i.e., it is its own transpose. We conjecture that this is because it can be obtained from the Vigenère tableau by a permutation that rearranges both rows and columns. Permutations can be represented as unitary matrices with exactly one 1 in each row and each column. We suspect that such a matrix *U* exists such that this tableau (*T*) can be obtained from the Vigenère tableau (*V*) by

$$T = U\,V\,U^{\mathrm{T}}$$

where the U on the left permutes the rows of the tableau, and its transpose on the right permutes the columns. The matrix *U* can be constructed using the base key. Determining how to do so is left as an exercise for the reader. Also, there are twenty-six ways to arrange the row of the tableau so that it is symmetric; are these the twenty-six rotations of the base key?

The fact that the tableau is symmetric may encourage you to think that it imposes a constraint on its member that we can exploit, but it does not. We will find that the columns that are unknown correspond exactly to the keys whose first letters are also unknown, so there is absolute freedom to shuffle those rows among them. In other words, this particular symmetry does not force us to choose any characters in the tableau.

Here again is Hamlet's soliloquy, encrypted with the Q3 using the base key and shift key `HAMLET`:

```
VAVBEFRABXEOIZQFWYUZQBTKIYBDECYCRXIWTZTWSTDFRVCCVCRSCCGZMWX
EJDIXIWUFTTMGCVXFUFHHALKTWZIFMWHOAMEFVOEBEFVABFQWCXHWDLCGEW
WZUDULKJTACGBWUJEKFRHBNLVYRRRTJJLDHXEHBDBLVXIDNTEBHXRFSHDLU
WBWIBBLVZOHRBSHVCRAAZTZUJIWCVXXIWVCMYVZRNEFWKTJSWITFTAXIZVQ
SBVVBYQBCFVABDVZFAEWXBQJBDECGDDLXJALBLFWYGAAJJHNTBWTUFRBLJH
YSBAUEDIJIZRMRXEHTDUSDRVCRVAGVCRVXOJAIDSJLJBWBWIBMMJWCZQOIZ
VNIBDBUUUHGTQDFAACYDQFYWUCCMKXINMMKJLGASEFVJSJEYAUCWWLBPRYV
UCOABWVIXRWWVIXRWLWFZBADJQJPBVPCFUSCJOAYWEXHVZCCEIQMVZVHHMY
BHDDUVWVIHQDLGCVXWGTTVALKJBURXITEBIBVGHXAOUTRRBAAUTACKRZRYW
LSJWURCPJLDNFSLUAYKCGEXTEJXHPRXIWAJFWJWAJJXIWBVALBWRMRLKTJQ
TJAZRNBAAGEOITVJLJBIDJBDEXRWTGBLKJLOEOEFVCJXDAIYFAACLDQDRGI
FYSCLLZQDVDWGRXXGQJPBZYVCUGDFIKMKQYRHQLZTWFXMDFGDSWFWCXBLMF
WVBFSHUHRFWKRNRVDNIJIHBYJDVYWJLJBXIWGXRFJTJYMSAJLGENDEVDIKA
ZVCBAAKRNTWGTXDIBJPHOEXURJXMSZVHYRGEKTVELWFCPRCBWTXRXXFRYNY
HSADAXIWYGSCDCGUURAGWYIFWVIXVBDFVCMWAYAFAOAVCPRXIZRQSHWTHZQ
BUGVCUXZWNVMOSTVAYXIKUMMTVPBDEJAHHZQSDAIMMODFGYMMXGCFSFSHVC
CWWVIVUXCMICCBEETDALBKVGMTCGUGWRBYINMBUNBZQXIWEJSBGZUZMMWVH
OZAWZRNRTWWTBIDVWUAYNUWCZNDWVCVXSEBIVBOCJLZQDVFIRUVJJLDTVGK
TXRTWGVOITDNTLUTJXHYRXIWRJHBEECMBDEC
```

Once again, we take the first fifty characters as a crib:

```
VAVBEF RABXEO IZQFWY UZQBTK IYBDEC YCRXIW TZTWST DFRVCC VC
tobeor nottob ethati sthequ estion whethe rtisno blerin th
```

This gives us the following incomplete key table:

	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		D			I									R				T	U	V			Y			
k_2								C				F			A				Y	Z						
k_3		V			R			Q	T											B						
k_4	F				B				D									V	W	X						
k_5								I	C					S	E		T			W						
k_6		O			W				Y					C	T			F			K					

We are going to multiply keys together, find new characters and new keys, until we can not long find any new knowledge about the tableau (not just the key table this time). The process should be automated, because it is long and tedious. But we will show you a few results, to give you an idea of how it goes. We might first square k_3, for example, to get

$$k_3^2 = \cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\mathtt{B}\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\cdot\mathtt{V}\cdot\cdot\cdot\cdot\cdot\cdot$$

We can match the result to k_1, since both have `V` in the `t` column:

k_1 = ·D··I········R···TUV··Y···
$k_3{}^2$ = ········B··········V······

Notice that $k_3{}^2$ has a B where k_1 has a gap. We can now augment k_1 with this new knowledge:

k_1 = ·D··I···B····R···TUV··Y···

If we multiply k_1 and k_4, we get something that we cannot match to one of the six keys, so we add a new key to the list:

$k_7 = k_1 \circ k_4$ = ····D·············Y·······

But we get a matching result if we multiply in the other order (as we should because of commutivity):

$k_7 = k_4 \circ k_1$ = ····D········V···X········

We can merge them together to get

k_7 = ····D········V···XY·······

We continue in this manner. Sometimes the list of keys will grow longer than twenty-six, but as more characters are uncovered, they can be merged. After nearly three thousand multiplications, most of which yield nothing new, we obtain the following mostly filled tableau. We have removed the labels on the left for the shift key letters, since we do not know how to assign keys to 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	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	C	D	F	L	·	·	E	A	·	·	I	·	Q	·	·	R	S	T	U	V	W	X	Y	Z	O
	C	D	F	·	I	·	·	L	B	·	N	A	·	R	H	·	S	T	U	V	W	X	Y	Z	O	·
	D	F	·	·	A	K	·	I	C	·	Q	B	·	S	E	·	T	U	V	W	X	Y	Z	O	·	H
	E	L	I	A	O	B	·	Z	H	·	F	·	·	·	X	·	K	·	N	Q	R	S	T	U	V	W
	F	·	·	K	B	·	·	A	D	·	R	C	·	T	L	·	U	V	W	X	Y	Z	O	·	H	E
	H	E	L	I	Z	A	·	Y	·	·	D	O	·	·	W	·	·	K	·	N	Q	R	S	T	U	V
	I	A	B	C	H	D	·	·	L	·	·	E	·	·	Z	·	N	Q	R	S	T	U	V	W	X	Y
	K	·	N	Q	F	R	·	D	·	·	U	·	·	W	B	·	X	Y	Z	O	·	H	E	L	I	A
	L	I	A	B	·	C	·	O	E	·	·	H	·	K	Y	·	·	N	Q	R	S	T	U	V	W	X
	N	Q	R	S	·	T	·	·	·	·	W	K	·	Y	D	·	Z	O	·	H	E	L	I	A	B	C
	O	·	H	E	X	L	·	W	Z	·	B	Y	·	D	U	·	F	·	·	K	·	N	Q	R	S	T
	Q	R	S	T	K	U	·	·	N	·	X	·	·	Z	F	·	O	·	H	E	L	I	A	B	C	D
	R	S	T	U	·	V	·	K	Q	·	Y	N	·	O	·	·	·	H	E	L	I	A	B	C	D	F
	S	T	U	V	N	W	·	·	R	·	Z	Q	·	·	·	·	H	E	L	I	A	B	C	D	F	·
	T	U	V	W	Q	X	·	N	S	·	O	R	·	H	K	·	E	L	I	A	B	C	D	F	·	·
	U	V	W	X	R	Y	·	Q	T	·	·	S	·	E	·	·	L	I	A	B	C	D	F	·	·	K
	V	W	X	Y	S	Z	·	R	U	·	H	T	·	L	N	·	I	A	B	C	D	F	·	·	K	·
	W	X	Y	Z	T	O	·	S	V	·	E	U	·	I	Q	·	A	B	C	D	F	·	·	K	·	N
	X	Y	Z	O	U	·	·	T	W	·	L	V	·	A	R	·	B	C	D	F	·	·	K	·	N	Q
	Y	Z	O	·	V	H	·	U	X	·	I	W	·	B	S	·	C	D	F	·	·	K	·	N	Q	R
	Z	O	·	H	W	E	·	V	Y	·	A	X	·	C	T	·	D	F	·	·	K	·	N	Q	R	S
	·	·	K	·	C	N	·	B	F	·	S	D	·	U	I	·	V	W	X	Y	Z	O	·	H	E	L
	·	H	E	L	Y	I	·	X	O	·	C	Z	·	F	V	·	·	·	K	·	N	Q	R	S	T	U
	·	K	·	N	D	Q	·	C	·	·	T	F	·	V	A	·	W	X	Y	Z	O	·	H	E	L	I
	·	N	Q	R	·	S	·	F	K	·	V	·	·	X	C	·	Y	Z	O	·	H	E	L	I	A	B

We pick off the six keys that match our original keys in any column to form our new key table:

	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	C	D	F		I			L	B		N	A		R	H		S	T	U	V	W	X	Y	Z	O	
k_2		K		N	D	Q		C			T	F		V	A		W	X	Y	Z	O		H	E	L	I
k_3	U	V	W	X	R	Y		Q	T			S		E			L	I	A	B	C	D	F			K
k_4	F			K	B			A	D		R	C		T	L		U	V	W	X	Y	Z	O		H	E
k_5	D	F			A	K		I	C		Q	B		S	E		T	U	V	W	X	Y	Z	O		H
k_6	Z	O		H	W	E		V	Y		A	X		C	T		D	F			K		N	Q	R	S

With the amplified key table, we can improve our decryption:

```
TOBEORNOTTOBETHATISTHEQUESTIONWHETHERTISNOBLERINTHE.IN.T.SU
F.ERTHESLIN..ANDARROWSOFOUTRA.EOUS.ORTUNEORTOTAKEAR.SA.A.NS
TASEAOF.ROU.LES.NDBYO..OSIN.EN..HE.TODIETOSLEE.NO.OREANDBYA
SLEE.TOSAYWEENDTHEHEARTA.HEANDTHETH.USANDNATUR.LSHOCKSTHATF
LESHISHEIRTOTISACONSU...TION.EVOU.LYTOBEW.SH..ODIETOSLEE..O
```

```
SLEE..ER.HAN.ETODREA.AYTHERE.THERUB.ORIN.H.TSLEE....EATHWHA
TDREA.S.AY.O.EWHENWEHAVESHU.FLED..F.H.S.ORT.L.OIL.UST.I.EUS
.AUSETHERESTHERES.ECTTHA....ES.ALA.I.YOFSOLON.LIFEF.RWHOW.U
LDBEARTHEWHI..ANDS.ORNSOF.I.ETHO..RES.ORSWRON.THE.ROUD.ANSC
ON.U.EL..HE.AN.SOFDI..RIZ.LO.ETHEL.WS.EL..THEINSOLEN.EOFO.F
I.EANDTHE..URNS.H.T.A.IENT.ER.TOF.HUNWORTH.TAKESWHENHEHI..E
LF.I.HTHISQU.ETU....EWITHA.AREB.DKINWHOWOULD.AR.ELSBEARTO.R
UNTANDSWEATUNDERAWE.RYLI.EBUT.H.TTHE.REA.O.S..E.H.N.AFTERDE
ATHTHEUNDIS.OVERE..OUNTRY.R..WHOSE.OURNNOTRA.ELLERRETURNS.U
ZZLESTHEW.LLAN..AKE.USRATHERBEARTH.SEILLSWEHA.ETHANFLYTOOTH
ER.THATWEKN.WNOTOFTHUS..NS.IEN.EDOTH.AKE..WAR.S..U.ALLANDTH
USTHENATI.EHUEOFRESOLUT..NI.S.CKLIED.ERWITHTHE..LE.AST..THO
U.HTANDENTER.RISESOF.REAT.ITHAND.O.ENTWI.HTHISRE.AR..HEIR.U
RRENT.TURNAWRYAN.LOSETHEN..EOFA.TION
```

Quite an improvement.

We are still working on finding a way to recover the base key from the tableau. We suspect that it will involve finding a matrix representation of an isomorphism into the Vigenère cipher.

Quagmire 4

Like the other quagmire ciphers, the quagmire 4 (Q4) can be factored [14]. In this case, there are two substitution keys, k_p on the plaintext side, and k_c on the ciphertext side, and one shift key (k_v):

$$Q_4\,(k_\mathrm{p}, k_\mathrm{c}, k_\mathrm{v}, t) \;=\; S\,(k_\mathrm{c}, V\,(k_\mathrm{v}', S^{-1}\,(k_\mathrm{p}, t)))$$

Now, k_v is the shift key, but k_v' is

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

Keys in Q4 are related to Vigenère rotations by

$$k \;=\; k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1}$$

This is *not* an isomorphism. Actually, we have a coset of a Q3 cipher. To see that, insert $e = k_\mathrm{p}^{-1} \circ k_\mathrm{p}$, which doesn’t change the product:

$$k \;=\; k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1} \;=\; k_\mathrm{c} \circ e \circ R_n \circ k_\mathrm{p}^{-1} \;=\; k_\mathrm{c} \circ (k_\mathrm{p}^{-1} \circ k_\mathrm{p}) \circ R_n \circ k_\mathrm{p}^{-1} \;=\; (k_\mathrm{c} \circ\; k_\mathrm{p}^{-1}) \circ (k_\mathrm{p} \circ R_n \circ k_\mathrm{p}^{-1})$$

The stuff in the first set of parentheses in the last right-hand side of the equation is just a constant permutation. The stuff in the second set is a Q3 key. So we see that we have a left coset of a Q3 cipher. But wait! It is also a right coset of a different Q3 cipher:

$$k \;=\; k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1} \;=\; k_\mathrm{c} \circ R_n \circ e \circ k_\mathrm{p}^{-1} \;=\; k_\mathrm{c} \circ R_n \circ (k_\mathrm{c}^{-1} \circ k_\mathrm{c}) \circ k_\mathrm{p}^{-1} \;=\; (k_\mathrm{c} \circ R_n \circ k_\mathrm{c}^{-1}) \circ (k_\mathrm{c} \circ\; k_\mathrm{p}^{-1})$$

So the Q4 is a left coset of the Q3 generated from k_p, and a right coset of the Q3 generated by k_c. Mathematicians like to use h to denote the multiplier for a coset. Notice that in our case, the multiplier on the left is the same as on the right, so we can write

$$h = k_\mathrm{c} \circ k_\mathrm{p}^{-1}$$

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? The good news is that *every* member of the Q4 tableau is an h for some Q3. Did we say “some Q3”? It turns out that they are all the same set of Q3 keys if we multiply on the left, and all the same as another Q3 if we multiply on the right. The tableaux may be shuffled a bit, but that is just an automorphism. To see why every member of Q4 is an h, take the inverse of some member of the Q4 and multiply it on the left to another member of the Q4 (remember that the inversion of a composition of permutations is a composition of the inverses in reverse order):

$$\begin{gathered}(k_\mathrm{c} \circ R_m \circ k_\mathrm{p}^{-1})^{-1} \circ (k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1}) = ((k_\mathrm{p}^{-1})^{-1} \circ R_m^{-1} \circ k_\mathrm{c}^{-1}) \circ (k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1}) \\ = k_\mathrm{p} \circ R_{-m} \circ k_\mathrm{c}^{-1} \circ k_\mathrm{c} \circ R_n \circ k_\mathrm{p}^{-1} = k_\mathrm{p} \circ R_{n-m} \circ k_\mathrm{p}^{-1}\end{gathered}$$

We obtain a member of a Q3 tableau. A similar result holds if we multiply on the right; in that case we get $k_\mathrm{c} \circ R_{n-m} \circ k_\mathrm{c}^{-1}$. The automorphism is reflected in the change in the rotation.

The strategy for key amplification is as follows: choose one of the partial keys from the table and invert it to get a partial h^{-1}. Multiply this by all other partial keys in the table. The products are now members of a Q3 tableau. We then apply the method for the quagmire 3 to them. When we have done that, we take the resulting partial keys and multiply by our chosen h. The results will overlap with the original key table, and we can merge them to improve our knowledge of the keys. We repeat the process of translating to the Q3, amplifying it, and translating back, until we gain no further knowledge.

Because the multiplication of two partial keys results in a product with fewer known letters than either of the inputs, we need to start with more knowledge than we needed in any of the other quagmires. This is no surprise, since the information content of a Q4 key is larger that that of a Q1, Q2, or Q3. In the present case we have, for a shift key of length m and two base keys,

$$I = m + 2 \log_{26} 26! = m + 37.6$$

This means that we need more knowledge about the key table if we are to reconstruct it as we did for the other quagmires.

Let’s see an example. Start with our favorite base key and add another:

k_c = `OPHELIABCDFGJKMNQRSTUVWXYZ`
k_p = `LADYMCBETHFGIJKNOPQRSUVWXZ`

Here is the tableau that they generate:

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

Our original *h* is

$$h = k_{\mathrm{c}} \circ k_{\mathrm{p}}^{-1} = \texttt{PAIHBFGDJKMOLNQRSTUCVWXYEZ}$$

and its inverse is

$$h^{-1} = \texttt{BETHYFGDCIJMKNLAOPQRSUVWXZ}$$

which appears in the tableau as the key for shift L.

Here is Hamlet's soliloquy encrypted with this Q4:

```
DAGYEZXAWRENISBBLJASBYWDIRWCEWCYERHGLSHQVTOCEPIWDYEKIWQSMQA
QRMURHGACHNQLNOJBXZHWVLPTYSUBQGHUVFEZDURYEZDAWBSGNQQQJRNBRQ
LKAMFLPALAXEGGAERHKBHDCLZJXIENOAGMQREPKMWLZIIMCNEVHQEBVPOZF
QGGIDWLZKEWEYVPDYEDFKLSFTHGNOJRHGDYMSZKXFRBLDLETQHTPKVRHKDG
TYZFKRBYIZDAWCZKPARQAVWEWCEWQMZLAAJZWLKGCBVDOAHFHYLTACEYTAH
RTYFHFMUTHKXHEREPLMFKJBDYEPFLDYEPANRAUCVAGEWQGGIDMFOGNSBVHK
DFUYJVANFXNTWMLDFWCMBBDGAYXFPIIFMFPAGBVKEZDETTEJJNXQLRKVESZ
HNUVYLFIQEQLFIQEQTGPSWDJAWEPYZONCFKIAEAKQEIHONMIQIGMPYFHWMS
```

```
GPOMFPLFIWBCTLNOJQNTLOVLPAKNERHTFDUYZLHQVVXTXIWDFHLAXHUKXRI
LVAYNEMCAGMCBVRAAKHILFQHZOIHVERHGJELQOGJEDRHGKOVLGGXHELPTRG
HTFKXFWDFLFUUNZAGEWAJAKMRRUGLBWLPAGURVEZDYDRJUIRLDFWGMBCULI
CKKIRGSBCZXYBERALWEPYYJDYFEJZITMHSJXWBLYTYCJFJZQMTQKGNQWLQZ
YOWBVPAWEBLDXFEPJMIEUXGJRMGSLAGEWRHGQQEBOTRRMKFAGBRGJQDMUHF
KDYWDFDXFHQNTMMUYOOHURRXBRQMKYFHREEEDLORLLZNVEMGGLQERAZXRCS
BEJMVRHGCBTMJWQNFJFLYRUBLFIQGYJZDYMQFJJCVVFFNVERHKXGTXLTHSB
YXLDYFRYGVOMVVTDAKRHDAHMNZOKMRTFPHSBKJUIHMVJZQRMFALNCTBVPDY
XQLFIOFRIYIYXYEQLMVLGDDBMNILABIJGJIFMYXMKSBRHGFETYNKASMFLFH
UNDLKXFENLGLDUCZGAAKGXGNSCCLFNOJKEVIOWVIAGSBCZZIIFPOAGMHPND
LQENLLDUUNJMLZFNOIHRERHGXEQYEQNHWCEW
```

Since we need more knowledge, and without enough of it the procedure will fail. Fifty characters are not enough for this example, so we take the first seventy-five characters as the crib:

```
DAGYEZ XAWREN ISBBLJ ASBYWD IRWCEW CYERHG LSHQVT
tobeor nottob ethati sthequ estion whethe rtisno

OCEPIW DYEKIW QSMQAQ RMURHG ACHNQL NOJ
blerin themin dtosuf ferthe slings and
```

This is the extent of our knowledge of the key table from this crib:

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

OK, so let's begin by choosing our multiplier as k_1:

$h = k_1$ = NO·QIR·······X···LAD··C···

Its inverse is

h^{-1} = S.WT····E··R·AB·DF·····N··

If we multiply this on the left of each of the Q4 keys, we have

	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
$h^{-1}\circ k_1$	A	B		D	E	F								N				R	S	T			W			
$h^{-1}\circ k_2$												W		B	S				F							
$h^{-1}\circ k_3$																										
$h^{-1}\circ k_4$									W					A					D	F						
$h^{-1}\circ k_5$							D		E											R	S					
$h^{-1}\circ k_6$		A				D													R		T					

It’s not much to work with: the first is naturally the identity, and we know nothing about the third. Nevertheless, we can apply the procedure for amplification of a Q3 key table and get

	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
$h^{-1}\circ k_1$	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
$h^{-1}\circ k_2$												W		B	S			D	F	G						
$h^{-1}\circ k_3$																										
$h^{-1}\circ k_4$									W					A	R				D	F	G					
$h^{-1}\circ k_5$							D		E											R	S					
$h^{-1}\circ k_6$		A				D	F		L			E							R	S	T					

We have added a few letters to the table. Now multiply each on the left by *h* to return to the Q4 key space:

	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	N	O		Q	I	R								X				L	A	D			C			
k_2												C		O	A			Q	R							
k_3																										
k_4									C					N	L				Q	R						
k_5							Q		I											L	A					
k_6		N				Q	R					I							L	A	D					

We acquired five new letters, highlighted in pink. We can merge this knowledge into our key table:

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

We proceed in this way, each time choosing a different h and whether to multiply h^{-1} on the right or left. In the end, we reach a state in which no new letters can be added. At that point, we have this key table:

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

That's quite an improvement. And, for this example, if we had been allowed 150 characters of crib, we could have filled all but the `c`, `j`, `v`, `x`, and `z` columns.

This is about all we have to say about the quagmire 4 cipher, so here is where the story ends.

Conclusion

We showed how the knowledge of a quagmire's key table can be amplified. A quagmire's base keys hold only so much information, so there is a lot of redundancy in a key table. The structure of the ciphers in light of group theory helps us to fill in missing information.

We hope you found all this useful, or at least interesting.

References

[1] American Cryptogram Association, The ACA and You, http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf, 2005. The 2016 version is archived at http://web.archive.org/web/*/http://cryptogram.org/docs/acayou16.pdf. The relevant pages are also available as http://www.cryptogram.org/downloads/aca.info/ciphers/QuagmireI.pdf, QuagmireII.pdf, QuagmireIII.pdf, and QuagmireIV.pdf.

[2] 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; http://archive.org/details/cryptanalysis00gain; chapter XVIII.

[3] 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.

[4] Saunders MacLane and Garrett Birkhoff, *Algebra*, 3rd edition, ISBN 978-0821816462.

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

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

[7] Gains, chapter XIV.

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

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

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

[11] James Lyons, Cryptanalysis of the Vigenere Cipher, Practical Cryptography website, 2012, http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-vigenere-cipher

[12] 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.

[13] 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.

[14] 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.