Quagmire ciphers and group theory: Recovering keywords from the key table

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

We demonstrate that with some ideas from group theory we are very often able to recover the keywords for a quagmire cipher from its key table. This would be the last task for a cryptologist in analyzing such a cipher.

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 permuted, or the ciphertext alphabet which slides against it is permuted, or both. Each of the twenty-six rows in the tableau for such a cipher as the key of a monoalphabetic substitution. A subset of them is chosen and applied in repeated sequence to the letters of the plaintext to create the ciphertext. That subset is what we call the "key table."

We start with the Vigenère cipher and work our way to the quagmire 4. For each, we demonstrate that it is very often possible to recover the keywords from the key table for each type of cipher. With the quagmires 1, 3, and 4, doing so utilizes some ideas from algebraic group theory. The process can mostly be automated, but in the end a human must choose from a small set of possibilities.

Vigenère cipher

Every alphabet key for the Vigenère cipher (V) is a rotation, which we denote as R_n for $n = 0, \ldots, 25$. Rotation leftward is taken as positive. The rows of the Vigenère tableau form a subgroup of the permutation group, where "multiplication" is the composition of permutations, and this subgroup is isomorphic to the integers modulo 26 (Z_{26}). Later we will need to know the orders of its elements, which we list here:

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

It is also important to note that there are twelve automorphisms of V, and that each corresponds to a different choice of order-26 element as the generator. Under each automorphism, the identity element $e = R_0$ is mapped to itself, as is R_{13}, which is the only order-2 element. Below is a table of examples of representations of these automorphisms, where we have organized them according to which rotation they map from R_1.

$$R_n = a_n \circ R_1 \circ a_n^{-1}$$

(Here and throughout this paper, the binary operation is the composition of permutations.) Note that these are not unique, and rotations of a have the same effect as a, since a rotated a_n is $a_n \circ R_m$ and

$$(a_n \circ R_m) \circ R_1 \circ (a_n \circ R_m)^{-1} = a_n \circ R_m \circ R_1 \circ R_{-m} \circ a_n^{-1} = a_n \circ R_1 \circ a_n^{-1}$$

Two of them, a_1 and a_{25}, are involutory. You might also notice that all of these are keys of affine ciphers that use an invertible multiplier (same as n) and no shift (any shift will also give automorphisms, $a_n \circ R_m$; see above).

n	a_n
1	ABCDEFGHIJKLMNOPQRSTUVWXYZ = e
3	ADGJMPSVYBEHKNQTWZCFILORUX
5	AFKPUZEJOTYDINSXCHMRWBGLQV
7	AHOVCJQXELSZGNUBIPWDKRYFMT
9	AJSBKTCLUDMVENWFOXGPYHQZIR
11	ALWHSDOZKVGRCNYJUFQBMXITEP
15	APETIXMBQFUJYNCRGVKZODSHWL
17	ARIZQHYPGXOFWNEVMDULCTKBSJ
19	ATMFYRKDWPIBUNGZSLEXQJCVOH
21	AVQLGBWRMHCXSNIDYTOJEZUPKF
23	AXUROLIFCZWTQNKHEBYVSPMJGD
25	AZYXWVUTSRQPONMLKJIHGFEDCB

Each a_n maps each R_m to $R_{m \cdot n}$, where $m \cdot n$ is evaluated modulo 26. The mathematician reading this may notice that while the Vigenère group $\{R_n\}$ with $\circ$ is isomorphic to the *additive* group Z_{26}, the set of automorphisms $\{a_n\}$ with $\circ$ *is* isomorphic to the *multiplicative* group Z_{26}^* of invertible elements of Z_{26}, as

$$a_m \circ a_n = a_{m \cdot n}$$

where m·n is integer multiplication modulo 26. We will need this table later, so be sure to memorize it now.

The order-13 elements, together with R_0, form a cyclic subgroup of their own (isomorphic to Z_{13}). One result of this fact is that we cannot obtain an order-26 element from the product of order-13 elements. Similarly, R_0 and R_{13} form a cyclic subgroup that is isomorphic to Z_2. From R_{13}, we can never obtain any of the order-26 or order-13 elements.

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. For 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
k_1	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_2	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
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	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
k_5	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_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
k_7	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

Quagmire 2

As we discussed earlier [4], the rows of a quagmire 2 (Q2) cipher's tableau form a left coset of the Vigenère subgroup. The base key for generating the tableau is the mixed alphabet formed by writing down the keyword, deleting repetitions of letters, and adding the remaining letters. For example, from the keyword ROUNDTABLE, we get

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

The fact that this is a left coset of the Vigenère is reflected in the fact that each key of the Q2 is a product of this base key with a rotation:

$$k = k_{\text{base}} \circ R_n$$

Finding the keywords for a Q2 is also quite easy. The shift key is in the leftmost column of the key table. Since each key is a rotation of the base key, we can read off the alphabetic keyword without difficulty. For example, the table for keywords `KNIGHTS` and `ROUNDTABLE` is

	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	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J
k_2	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U
k_3	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H
k_4	G	H	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F
k_5	H	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G
k_6	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D
k_7	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q

Quagmire 1

We also saw earlier [4] that the quagmire 1 (Q1) cipher forms a coset of the Vigenère, but this time on the right:

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

If we invert a Q1 key, we get an element of a left coset, i.e., a Q2 key:

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

So the strategy to recover the alphabetic keyword is to invert the rows of the key table and then read off the keyword as we did for the quagmire 2.

Our example uses the same two keywords as above. The Q1 key table is

	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	K	L	O	I	N	P	Q	R	S	T	U	M	V	H	F	W	X	E	Y	J	G	Z	A	B	C	D
k_2	N	O	R	L	Q	S	T	U	V	W	X	P	Y	K	I	Z	A	H	B	M	J	C	D	E	F	G
k_3	I	J	M	G	L	N	O	P	Q	R	S	K	T	F	D	U	V	C	W	H	E	X	Y	Z	A	B
k_4	G	H	K	E	J	L	M	N	O	P	Q	I	R	D	B	S	T	A	U	F	C	V	W	X	Y	Z
k_5	H	I	L	F	K	M	N	O	P	Q	R	J	S	E	C	T	U	B	V	G	D	W	X	Y	Z	A
k_6	T	U	X	R	W	Y	Z	A	B	C	D	V	E	Q	O	F	G	N	H	S	P	I	J	K	L	M
k_7	S	T	W	Q	V	X	Y	Z	A	B	C	U	D	P	N	E	F	M	G	R	O	H	I	J	K	L

The inverses are

	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
$k_1{}^{-1}$	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V
$k_2{}^{-1}$	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P
$k_3{}^{-1}$	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X
$k_4{}^{-1}$	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X	Y	Z
$k_5{}^{-1}$	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H	I	J	K	M	P	Q	S	V	W	X	Y
$k_6{}^{-1}$	H	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G
$k_7{}^{-1}$	I	J	K	M	P	Q	S	V	W	X	Y	Z	R	O	U	N	D	T	A	B	L	E	C	F	G	H

Quagmire 3

The quagmire 3 keys form a subgroup of permutations that is isomorphic to the Vigenère [4]. This isomorphism is expressed in terms of the base key as

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

Now, it is well known and easy to prove that any permutation can be rewritten as a product of exchanges. An exchange simply swaps two elements. Since we can get from the identity element to any permutation by exchanges, it follows that we can get from any permutation to another permutation. After all, we could first go from the first to the identity, then on to the second. In the case of alphabetic keys, we can do this with twenty-five or fewer exchanges.

Our strategy for recovering the base key is to find a sequence of exchanges that will transform one of the order-26 elements of the Q3 table into a rotation of order 26, which we choose to be R_1. The product of those exchanges is a base key. (The mathematician in the audience may prefer to do it by diagonalizing matrices.) Since the exchanges are applied to both sides of a key, they move around more than just two letters. Therefore it is best to start at one end and work our way to the other. The base key that we find may not be the one we want (up to a rotation), so we will use the automorphisms of the Vigenère to find eleven additional candidate base keys. We then have to pick out the best one by eye.

Unfortunately, if we start with an order-13 key, then we are unlikely to succeed. The reason for this is that there are many Q3 ciphers with the same order-13 elements. If we try to find an isomorphism that takes R_2 to our order-13 Q3 key, we are able to do so. However, when we use the result to find an order-26 generator, there are many possibilities. Each of them generates a Q3 with the same order-13 elements, but with different order-26 elements. Even with the automorphisms of the Vigenère, we are unlikely to find the base key that we seek. A similar thing happens if we start with the order-2 element. Recall that the order-13 elements of the Vigenère with R_0 form a subgroup, and that from it we are unable to obtain any of the order-26 elements. Similarly for the subgroup $\{R_0, R_{13}\}$. The isomorphism from V to Q3 does not change this structure.

If we randomly select an element from a Q3 tableau, there is a 6/13 = 46% chance that we will have an order-26 element. For a key table with two elements, the odds are $1 - (7/13)^2 = 71\%$. Clearly, for a table of n keys, the chances of finding an order-26 element is $1 - (7/13)^n$. So there is good reason to be optimistic.

The method will be made more clear by an example. Here is a key table built from with the shift keyword `KNIGHTS`. The shift key is in the column under `r`, indicating that the base key begins with `R`.

	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	X	R	S	Z	O	U	N	D	T	A	Y	B	Q	M	L	E	K	C	V	P	F	G	H	I	J
k_2	E	C	H	B	G	I	J	K	M	P	Q	F	S	A	D	V	W	N	X	L	T	Y	Z	R	O	U
k_3	S	V	Y	P	X	Z	R	O	U	N	D	W	T	M	J	A	B	I	L	Q	K	E	C	F	G	H
k_4	P	Q	W	K	V	X	Y	Z	R	O	U	S	N	J	H	D	T	G	A	M	I	B	L	E	C	F
k_5	Q	S	X	M	W	Y	Z	R	O	U	N	V	D	K	I	T	A	H	B	P	J	L	E	C	F	G
k_6	F	G	J	E	I	K	M	P	Q	S	V	H	W	L	A	X	Y	T	Z	C	B	R	O	U	N	D
k_7	R	O	D	Y	N	T	A	B	L	E	C	U	F	X	V	G	H	S	I	Z	W	J	K	M	P	Q

The orders of these keys are 13, 26, 13, 13, 2, 26, and 13. Let us concentrate first on k_2, since it has order 26. We need to find exchanges which eventually convert k_2 into R_1. For each exchange, we transform the key thusly:

$$k \;\rightarrow\; E\,k\,E^{-1} \;\;(=\; E\,k\,E)$$

We are always able to succeed with at most twenty-five exchanges. Here is one example of a series of exchanges (this series is not unique):

k_1 =	ECHBGIJKMPQFSADVWNXLTYZROU	
$\rightarrow$	BGHECIJKMPQFSADVWNXLTYZROU	$E_{2,5}$
$\rightarrow$	BCJEGIHKMPQFSADVWNXLTYZROU	$E_{3,7}$
$\rightarrow$	BCDPGIHKMEQFSAJVWNXLTYZROU	$E_{4,10}$
$\rightarrow$	BCDEVIHKMPQFSAJGWNXLTYZROU	$E_{5,16}$
$\rightarrow$	BCDEFYHKMPQVSAJGWNXLTIZROU	$E_{6,22}$
$\rightarrow$	BCDEFGOKMPQVSAJYWNXLTIZRHU	$E_{7,25}$
$\rightarrow$	BCDEFGHJMPQVSAKYWNXLTIZROU	$E_{8,15}$
$\rightarrow$	BCDEFGHIPMQVSAKYWNXLTJZROU	$E_{9,10}$
$\rightarrow$	BCDEFGHIJYQVSAKMWNXLTPZROU	$E_{10,16}$
$\rightarrow$	BCDEFGHIJKOVSAYMWNXLTPZRQU	$E_{11,25}$
$\rightarrow$	BCDEFGHIJKLYSAVMWNXOTPZRQU	$E_{12,15}$
$\rightarrow$	BCDEFGHIJKLMQAVYWNXOTPZRSU	$E_{13,25}$
$\rightarrow$	BCDEFGHIJKLMNWVYAQXOTPZRSU	$E_{14,17}$
$\rightarrow$	BCDEFGHIJKLMNOZYAQXWTPVRSU	$E_{15,23}$
$\rightarrow$	BCDEFGHIJKLMNOPUAQXWTZVRSY	$E_{16,26}$
$\rightarrow$	BCDEFGHIJKLMNOPQTUXWAZVRSY	$E_{17,21}$
$\rightarrow$	BCDEFGHIJKLMNOPQRWXUAZVTSY	$E_{18,20}$
$\rightarrow$	BCDEFGHIJKLMNOPQRSVUAZXTWY	$E_{19,23}$
$\rightarrow$	BCDEFGHIJKLMNOPQRSTZAUXVWY	$E_{20,22}$
$\rightarrow$	BCDEFGHIJKLMNOPQRSTUYZXVWA	$E_{21,26}$
$\rightarrow R_1$ =	BCDEFGHIJKLMNOPQRSTUVWXYZA	$E_{22,25}$

The product of the exchanges is our provisional base key:

$$k_{\text{base}}' = E_{2,5} \circ E_{3,7} \circ \ldots \circ E_{21,26} \circ E_{22,25} = \texttt{AEGJPVYODBCHKQWZUTLFIMSXRN}$$

We have not found the base key that we seek, since we do not see a discernable keyword in it. Therefore, we apply the twelve automorphisms of the Vigenère group. For each, we multiply by a_n on the right (since the automorphism is on the rotations). These are the twelve candidates that we get:

```
AEGJPVYODBCHKQWZUTLFIMSXRN
AJYBKZLMREPOCQUFSNGVDHWTIX
AVCZINPBWFRJDQLXGOKTSEYHUM
AOWMGBUXPHLNYQIEDZSJCTRVKF
ABLECFGHIJKMPQSVWXYZROUNDT
AHSOLJWNCMYTGQRBIVUEKXDFPZ
AZPFDXKEUVIBRQGTYMCNWJLOSH
ATDNUORZYXWVSQPMKJIHGFCELB
AFKVRTCJSZDEIQYNLHPXUBGMWO
AMUHYESTKOGXLQDJRFWBPNIZCV
```

```
AXITWHDVGNSFUQCOPERMLZKBYJ
ANRXSMIFLTUZWQKHCBDOYVPJGE
```

We can clearly see a recognizable keyword in $k_{\text{base}}' \circ a_9$:

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

Now, rotating the base key merely reorders the rows of tableau but does not change them:

$$k_{\text{base}} \rightarrow k_{\text{base}} \circ R_m$$

$$\begin{aligned} k_n = k_{\text{base}} \circ R_n \circ k_{\text{base}}^{-1} \rightarrow & (k_{\text{base}} \circ R_m) \circ R_n \circ (k_{\text{base}} \circ R_m)^{-1} \\ = & \ k_{\text{base}} \circ R_m \circ R_n \circ R_{-m} \circ k_{\text{base}}^{-1} \\ = & \ k_{\text{base}} \circ R_n \circ k_{base}^{-1} = k_n \end{aligned}$$

Therefore, we can harmlessly rotate k_{base} until it begins with `R`, as we know from above that it must. We now have it and the keyword:

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

Quagmire 4

The alphabetic keys of the quagmire 4 cipher (Q4) are constructed from rotations with two base keys, one on the plaintext side (k_{p}), and one on the ciphertext side (k_{c}):

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

As we have seen [4], the Q4 is both a left coset and a right coset of Q3 ciphers (different on each side). The multiplier that takes us from the Q3 to the Q4 is

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

To go from Q4 to the Q3 on the left, we multiply the Q4 keys on the left by the inverse of h:

$$h^{-1} \circ k = k_{\text{p}} \circ R_n \circ k_{\text{p}}^{-1}$$

and to go to the Q3 on the right, we multiply by h^{-1} on the right:

$$k \circ h^{-1} = k_{\text{c}} \circ R_n \circ k_{\text{c}}^{-1}$$

We also saw that *any* row of the key table can serve as an h. So our strategy for recovering the keywords is to choose an h and then to transform the key table to the left Q3. There we can employ the technique above to recover k_{p}. Transforming the key table to the right Q3 will allow us to find k_{c}.

Here is an example, built from three different keywords. Once again, we can see that the shift key, k_{v} = `KNIGHTS`, appears in the column under `r`; this indicates that k_{p} begins with the letter `R`.

	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	T	Y	P	W	Z	E	X	C	A	L	V	I	O	M	B	U	K	R	Q	N	D	F	G	H	J
k_2	V	W	E	S	Z	X	C	A	L	I	B	Y	U	Q	O	R	D	N	F	T	P	G	H	J	K	M
k_3	G	H	M	D	K	N	O	P	Q	S	T	J	V	R	B	W	Y	I	Z	F	U	E	X	C	A	L
k_4	O	P	T	M	S	V	W	Y	Z	E	X	Q	C	K	H	A	L	G	I	N	J	B	U	R	D	F
k_5	P	Q	V	N	T	W	Y	Z	E	X	C	S	A	M	J	L	I	H	B	O	K	U	R	D	F	G
k_6	X	C	I	Z	L	B	U	R	D	F	G	A	H	Y	V	J	K	T	M	E	W	N	O	P	Q	S
k_7	E	X	L	Y	A	I	B	U	R	D	F	C	G	W	T	H	J	S	K	Z	V	M	N	O	P	Q

Suppose we choose k_1 to be our h.

$$h = k_1 = \texttt{JPIVGWXYMZRKOUNDTSABQLEHCF}$$

Let us use it to transform the key table into the Q3 on the left:

	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
$k_1^{-1} \circ k_1$	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
$k_1^{-1} \circ k_2$	L	E	G	A	F	H	I	J	K	M	P	C	Q	T	N	S	V	U	W	B	D	X	Y	Z	R	O
$k_1^{-1} \circ k_3$	X	Y	O	V	R	U	N	D	T	A	B	Z	L	S	P	E	C	M	F	W	Q	G	H	I	J	K
$k_1^{-1} \circ k_4$	N	D	B	O	A	L	E	C	F	G	H	T	I	R	Y	J	K	X	M	U	Z	P	Q	S	V	W
$k_1^{-1} \circ k_5$	D	T	L	U	B	E	C	F	G	H	I	A	J	O	Z	K	M	Y	P	N	R	Q	S	V	W	X
$k_1^{-1} \circ k_6$	H	I	M	F	K	P	Q	S	V	W	X	J	Y	C	L	Z	R	B	O	G	E	U	N	D	T	A
$k_1^{-1} \circ k_7$	G	H	K	C	J	M	P	Q	S	V	W	I	X	E	B	Y	Z	A	R	F	L	O	U	N	D	T

Notice that the shift key has been transformed to its encryption by a monoalphabetic substitution cipher using h as its key. Again it appears in column `r`.

$$S(h, k_v) = \texttt{RUMXYBA}$$

Fortunately, $k_1^{-1} \circ k_3$ has order 26, and we can use it. We obtain this provisional base key:

$$k_{\text{base}}' = \texttt{AXITWHDVGNSFUQCOPERMLZKBYJ}$$

Since no discernable keyword pops out at us, we try the automorphisms of V. The best choice is a_{23}, and we obtain

$$k_{\text{base}}' \circ a_{23} = \texttt{ABLECFGHIJKMPQSVWXYZROUNDT}$$

After a harmless rotation, we have found the base key and keyword on the plaintext side:

$$k_p = \texttt{ROUNDTABLECFGHIJKMPQSVWXYZ}$$

Next, we work with the Q3 on the right:

	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
$k_1 \circ k_1^{-1}$	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
$k_2 \circ k_1^{-1}$	I	R	L	G	C	H	J	K	U	M	N	B	O	P	Q	S	T	F	V	W	D	Y	Z	A	E	X
$k_3 \circ k_1^{-1}$	S	W	Q	E	O	X	C	A	V	L	I	T	B	U	R	D	F	Z	G	H	Y	J	K	P	M	N
$k_4 \circ k_1^{-1}$	E	A	Z	B	W	U	R	D	C	F	G	X	H	J	K	M	N	I	O	P	L	Q	S	Y	T	V
$k_5 \circ k_1^{-1}$	X	L	E	U	Y	R	D	F	A	G	H	C	J	K	M	N	O	B	P	Q	I	S	T	Z	V	W
$k_6 \circ k_1^{-1}$	F	J	D	N	U	O	P	Q	H	S	T	G	V	W	Y	Z	E	M	X	C	K	A	L	R	I	B
$k_7 \circ k_1^{-1}$	D	H	R	M	B	N	O	P	G	Q	S	F	T	V	W	Y	Z	K	E	X	J	C	A	U	L	I

We can see the shift key in the column under k, but here it does not mean that the keyword begins with K. However, if it means anything,

$$S\,(h, \text{“k”}) \;=\; \text{“R”}$$

As expected, $k_3 \circ k_1^{-1}$ has order 26. Using it we can obtain this provisional base key (as an example):

$$k_{\text{base}}' \;=\; \texttt{ASGCQFXPDEORZNUYMBWKIVJLTH}$$

The best automorphism seems again to be a_{23}.

$$k_{\text{base}}' \circ a_{23} \;=\; \texttt{ALIBURDFGHJKMNOPQSTVWYZEXC}$$

After a harmless rotation, we have found the base key and likely keyword on the ciphertext side:

$$k_{\text{c}} \;=\; \texttt{EXCALIBURDFGHJKMNOPQSTVWYZ}$$

We now know everything about this Q4 cipher.

Conclusion

We have shown how it is often possible to recover the keywords for a quagmire cipher from its key table. To do so, we used some ideas from group theory. The techniques are mostly algorithmic and do not require guessing or dictionary attacks, but do require human intervention in deciding from among a small number of results.

Appendix: Identifying the cipher

Suppose that we have a key table k_1, k_2, ..., and we know that it belongs to a cipher in the V-Q family. Can we determine which one? Yes. And we only need two distinct keys to do it. Call them k_1 and k_2.

If we have two keys and at least one of them is a rotation (one may be the identity e = R_0), then the cipher is a Vigenère. If not, then continue as follows.

The keys of a Q1 are all of the form

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

Therefore, if we take $k_1 \circ k_2^{-1}$ and obtain a rotation, then we know we have a Q1 cipher.

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

The keys of a Q2 are of the form

$$k = k_{\text{base}} \circ R_n$$

So, if we take $k_1^{-1} \circ k_2$ and obtain a rotation, then we know we have a Q2 cipher.

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

If we still do not know, then find the order of the keys. If they are both in the set {1,2,13,26}, then we are confident that we have a Q3. Furthermore, if one is the identity and the other is not a rotation, then that indicates a Q3.

If all of the above tests have failed, then find $k_1 \circ k_2^{-1}$ and $k_1^{-1} \circ k_2$. If they both pass the Q3 test, then the cipher is Q4.

Appendix: Further examples

On page 183 of Gaines's book [2], in figure 148, are five exercises in keyword recovery. Let's see what we can do with them.

1. `Q·ZAXBOCN·ERFPVG·YMUI·W·TL` (Q1)

The key has some missing letters. Nevertheless, we can invert it to find

`DFH·KMP·U··ZSIGNAL·YTOWERC`

The keyword is clearly `SIGNALBYTOWER`.

2. `UVDWSXKYHZCFRJQLINGPTOMEAB` (Q3)

Nicely, this key has order 26. From that alone, we know that it belongs to a quagmire 3, and did not have to be told. By whatever method is most expedient, we obtain, for example, this provisional base key:

$$k_{\text{base}}' = \texttt{AUTPLFXESGKCDWMRNJZBVOQIHY}$$

Multiplying on the right by a_{19} (one of the automorphisms of the Vigenère group) gives

$$k_{\text{base}}' \circ a_{19} = \texttt{ABDFHJKPQRSUVWXYZCLINGTOME}$$

An irrelevant rotation gives us the original base key with obvious keyword:

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

3. `HJGKFPEQORSTDMBUVWXAYZCLIN` (Q3)

The order of this key is 13, so there is little that we can do with it alone. However, one might notice that if we take the key from example 2 and raise it to the 24$^{\text{th}}$ power, we obtain this key. They belong to the same Q3 tableau, so have the same keyword, `CLINGTOME`.

4. `VNUXJYZDQEMPOWCKRIATLSBFGH`
   `HSGJRKLNFPQBUIVAWCXYTZDEMO` (Q4)

The inverse of the first multiplied on the left of the second gives

$$k_1^{-1} \circ k_2 = \texttt{ZVYEQPUBXLIWCRASNODFTGHJKM}$$

This element has order 26. From it we can find a provisional base key like this one:

$$k_{\text{base}}' \;=\; \texttt{AZMCYKIXJLWHBVGUTFPSDEQNRO}$$

Multiplying on the right by a_{23} gives

$$k_{\text{base}}' \circ a_{23} \;=\; \texttt{ANDFGHJKMOQSTVWXYZREPUBLIC}$$

An irrelevant rotation gives us the original base key with obvious keyword:

$$k_{\text{p}} \;=\; \texttt{REPUBLICANDFGHJKMOQSTVWXYZ}$$

When we multiply the inverse of the first key on the right of the second we have

$$k_2 \circ k_1^{-1} \;=\; \texttt{XDVNPEMOCRATQSUBFWZYGHIJKL}$$

Again (no surprise) we have an element with order 26. We can find a provisional base key such as this one:

$$k_{\text{base}}' \;=\; \texttt{AXJRWICVHOUGMQFEPBDNSZLTYK}$$

Multiplying on the right by a_{23} gives

$$k_{\text{base}}' \circ a_{23} \;=\; \texttt{ATSBFGHIJKLNPQUVWXYZDEMOCR}$$

An irrelevant rotation gives us the original base key with obvious keyword:

$$k_{\text{c}} \;=\; \texttt{DEMOCRATSBFGHIJKLNPQUVWXYZ}$$

5. `GXYZMHAFTRLKEVQUOJWIPNSBCD`
   `E·GJIK·LB··UTCVW·QDXS·····` (Q3)

The first key has order 2, which makes it useless by itself. However, we can use it to fill in missing letter in the second key. If we apply the key amplification method from [4], we find that in order to be consistent with the first key, the second must be (with still two missing letters)

`E·GJIKMLBOPUTCVWNQDXSYZ·AR`

The missing letters are `F` and `H`. One choice of placing them results in an order-13 key. Since that cannot help us, we try the other choice:

`EFGJIKMLBOPUTCVWNQDXSYZHAR`

This key has order 26, as desired. From it we can find a provisional base key such as this one:

$$k_{\text{base}}' \;=\; \texttt{AEIBFKPWZRQNCGMTXHLUSDJOVY}$$

Multiplying on the right by a_9 gives

$$k_{\text{base}}' \circ a_9 = \texttt{ARLEQUINSBCDFGJKMOPTVWXYZH}$$

Then we can harmlessly rotate to get the intended base key and its keyword:

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

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] Thomas Kaeding, Quagmire ciphers, group theory, and information: Key amplification in crib-based attacks, Cryptology ePrint Archive, report 2022/1382.