Quagmire ciphers and group theory: What is a Beaufort cipher?

Thomas Kaeding
xnrqvat@oynpxfjna.qhpxqaf.bet (to combat spam, my email has been ROT13'ed)
October, 2022

We show that a Beaufort cipher is simultaneously both a quagmire 1 and a quagmire 2 cipher, which includes it in the set of quagmire 4 ciphers as well, albeit as a degenerate one. The Beaufort is one of a family of ciphers that share this property.

Introduction

The Beaufort cipher [1, 2] is a periodic polyalphabetic substitution cipher. It is an involution, meaning that it is its own inverse, and the decryption process is identical to the encryption process.

$$\begin{aligned} c &= B(k, p) \\ p &= B^{-1}(k, c) = B(k, c) \end{aligned}$$

The key k here is a list of letters, similar to the key of the Vigenère cipher [3]. If the key has length L and we think of each letter as the number representing its place in the alphabet (A=0, B=1, ...), then the action of the cipher on each letter of the plaintext p and ciphertext c is

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

The quagmire ciphers [1, 2] (also known as type 1, 2, 3, and 4 periodic polyalphabetic substitution ciphers) are generalizations of the Vigenère cipher in which the plaintext alphabet is permuted, or the ciphertext alphabet is permuted, or both. Each of the twenty-six rows in the tableau for such a cipher is the key of a monoalphabetic substitution. All such keys are members of the permutation group of 26 objects. We saw earlier [4] that the keys in the tableaux of the quagmire ciphers form a subgroup isomorphic to the Vigenère in the case of Q3, or cosets of V for the Q1 and Q2. The quagmire 4 is a coset of a Q3 cipher. We also saw [5] that the isomorphisms of the Vigenère are the affine cipher keys.

We intend to show how the Beaufort cipher is one of a family of ciphers built as quagmire ciphers with the affine cipher keys. One interesting property that they share is that each is simultaneously both a Q1 and Q2 cipher. In the case of the Beaufort, we argue that it is the polyalphabetic cipher as far from the Vigenère as possible.

A few things about the Vigenère

The members (keys) in the V tableau are rotations, $\{R_n\}$, where we take n to be the number of steps to the left in the rotation of the alphabet. They form a subgroup isomorphic to the set of integers

modulo 26 with addition(Z_{26}). The binary operation in the group of permutation is the usual composition of permutations (even if we call it “multiplication” often). Here, the rotations add:

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

Arithmetic in the subscripts throughout this paper are done modulo 26.

The automorphisms of the Vigenère group are these:

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 = b_{25}

They are numbered by how they transform R_1:

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

It is interesting that $\{a_n\}$ form a group of their own that is isomorphic to Z_{26}^*, which is the set of invertible elements of Z_{26} under multiplication. As permutations, however, they use the same operation as the rotations of the Vigenère. But here,

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

The first one, a_1, is the unmixed alphabet, and is the identity permutation e. It is a member of all subgroups, and in V we call it R_0. The last one is also called b_{25}, but you have to wait to find out why.

An important fact about the permutations a_n is that, while any permutation when multiplied by a rotation on the right is merely rotated, the affine permutations have the same property when multiplied on the left by an R. For example,

$$a_{21} \circ R_5 = \text{BWRMHCXSNIDYTOJEZUPKFAVQLG}$$

and

$$R_5 \circ a_{21} = \text{FAVQLGBWRMHCXSNIDYTOJEZUPK}$$

The size of the resulting rotation in the second is not a simple combination of the subscripts on *a* and *R*. A general permutation does not have this property and will be deranged when multiplied by a rotation on its left. For example, even a simple exchange is altered:

$$R_5 \circ E_{1,2} = E_{6,7} \circ R_5$$

The keys of the Beaufort

Recall that the identity element of the group of permutations is

$$e = \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ}$$

The permutation that reverzes the alphabet is the also the key of the Atbash cipher [6]:

$$z = \texttt{ZYXWVUTSRQPONMLKJIHGFEDCBA}$$

Rotations of *z* are the keys of the Beaufort. We may as well include the tableau, for otherwise this paper would be too short.

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	name
A	A Z Y X W V U T S R Q P O N M L K J I H G F E D C B	b_{25}
B	B A Z Y X W V U T S R Q P O N M L K J I H G F E D C	b_{24}
C	C B A Z Y X W V U T S R Q P O N M L K J I H G F E D	b_{23}
D	D C B A Z Y X W V U T S R Q P O N M L K J I H G F E	b_{22}
E	E D C B A Z Y X W V U T S R Q P O N M L K J I H G F	b_{21}
F	F E D C B A Z Y X W V U T S R Q P O N M L K J I H G	b_{20}
G	G F E D C B A Z Y X W V U T S R Q P O N M L K J I H	b_{19}
H	H G F E D C B A Z Y X W V U T S R Q P O N M L K J I	b_{18}
I	I H G F E D C B A Z Y X W V U T S R Q P O N M L K J	b_{17}
J	J I H G F E D C B A Z Y X W V U T S R Q P O N M L K	b_{16}
K	K J I H G F E D C B A Z Y X W V U T S R Q P O N M L	b_{15}
L	L K J I H G F E D C B A Z Y X W V U T S R Q P O N M	b_{14}
M	M L K J I H G F E D C B A Z Y X W V U T S R Q P O N	b_{13}
N	N M L K J I H G F E D C B A Z Y X W V U T S R Q P O	b_{12}
O	O N M L K J I H G F E D C B A Z Y X W V U T S R Q P	b_{11}
P	P O N M L K J I H G F E D C B A Z Y X W V U T S R Q	b_{10}
Q	Q P O N M L K J I H G F E D C B A Z Y X W V U T S R	b_9
R	R Q P O N M L K J I H G F E D C B A Z Y X W V U T S	b_8
S	S R Q P O N M L K J I H G F E D C B A Z Y X W V U T	b_7
T	T S R Q P O N M L K J I H G F E D C B A Z Y X W V U	b_6
U	U T S R Q P O N M L K J I H G F E D C B A Z Y X W V	b_5
V	V U T S R Q P O N M L K J I H G F E D C B A Z Y X W	b_4
W	W V U T S R Q P O N M L K J I H G F E D C B A Z Y X	b_3
X	X W V U T S R Q P O N M L K J I H G F E D C B A Z Y	b_2
Y	Y X W V U T S R Q P O N M L K J I H G F E D C B A Z	b_1
Z	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A	$b_0 = z$

We have numbered them by the number of leftward shifts of z. For a leftward shift, we multiply by the corresponding rotation on the right, or the inverse rotation on the left:

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

Notice that the individual keys are involutory, like the full cipher:

$$b_n^2 = z^2 = e$$

One way in which the Beaufort is as far from the Vigenère as possible is that z is the furthest permutation from e. The swap of any two letters brings it closer to e. Another way is that the Vigenère has the Z_{26} group structure, with many elements having order 26, whereas the Beaufort has lost that group structure (it is not even closed) and all its elements have order 2.

The composition of two bs is antisymmetric. When we multiply them in one order they give a rotation, but in the other order they give the inverse rotation. This equation summarizes that fact and more:

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

The composition of a b with a rotation is another b:

$$b_m \circ R_n = b_{m+n}$$
$$R_n \circ b_m = b_{m-n}$$

And, finally, the composition of a b with an a is another a, rotated:

$$b_m \circ a_n = a_{-n} \circ R_q$$
$$a_n \circ b_m = a_{-n} \circ R_s$$

where q and s are some numbers that depend on m and n.

The reversal z is also an automorphism of V:

$$R_n \rightarrow z \circ R_n \circ z^{-1} = z \circ R_n \circ z = R_{-n}$$

If you are wondering why z does not appear in the table of automorphisms above, you can stop worrying about it. It is the last line, disguised as $a_{25} = b_{25}$. The rotation between it and z does not matter:

$$a_{25} \circ R_n \circ a_{25}^{-1} = b_{25} \circ R_n \circ b_{25}^{-1} = (z \circ R_{25}) \circ R_n \circ (z \circ R_{25})^{-1} = z \circ R_{25} \circ R_n \circ R_{-25} \circ z = z \circ R_n \circ z$$

By the same argument, all of the bs provide the same isomorphism of V.

The Beaufort is a quagmire

To see that the Beaufort cipher is a quagmire 1, we only have to show that every one of its keys is of the form

$$b_n = R_m \circ k_{\text{base}}^{-1}$$

where k_{base} is the base key of the Q1 (the mixed alphabet on the plaintext side, usually made from a keyword) and m is not necessarily the same as n. In other words, we need to show that the Beaufort is a right coset of the Vigenère. Well, we already have this, from an equation above:

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

Thus, B is a Q1, and its base key is z.

To see that B is also a Q2, we need its keys to be of the form

$$b_n = k_{\text{base}} \circ R_m$$

so that the B is a left coset of V. We have that already also, in this equation from above:

$$b_n = z \circ R_n$$

Once again, the base key is z. This is all very simple, eh?

The sets of Q1 and Q2 ciphers are subset of the set of quagmire 4 ciphers. Therefore, the Beaufort is also a Q4. However, it is a degenerate one, since one of its base keys is the identity permutation:

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

Family of periodic affine ciphers

We can construct a small family of ciphers that share this property that they are simultaneously Q1 and Q2 ciphers. We begin with the automorphisms of the Vigenère that we saw earlier. Suppose we build a Q2 using one affine key (a_m, say) as the base key; each key of this cipher has the form

$$k_n = a_m \circ R_n$$

Each of these keys is a rotation of a_m leftward by n steps. Can we build a Q1 cipher with the same set of keys? Yes:

$$k_n = R_n \circ a_m$$

This Q2 has base key a_m^{-1}. The k_n may be in a different order in the tableau than they were for the Q1, but they are all there. This only works because $R_n \circ a_m$ is a rotation of a_m. For some other permutation, composition with a rotation on the left does not generally result in a simple rotation of the permutation.

So what we have is a family of twelve “periodic affine ciphers.” At one end, $a_1 = e$ gives the Vigenère cipher, while at the other end, $a_{25} = b_{25}$ give the Beaufort. Each of them is simultaneously a Q1 and Q2 cipher.

Beaumire Quagfort ciphers

Is there any point in building the analog of quagmire ciphers from the Beaufort rather than from the Vigenère? We might try some options like the four quagmire types, where we replace the rotations of V with the keys of B:

type 1: $k_n = b_n \circ k_{\text{base}}^{-1}$
type 2: $k_n = k_{\text{base}} \circ b_n$
type 3: $k_n = k_{\text{base}} \circ b_n \circ k_{\text{base}}^{-1}$
type 4: $k_n = k_C \circ b_n \circ k_P^{-1}$

There is no reason to do any of these, because they can all be rewritten as quagmire ciphers:

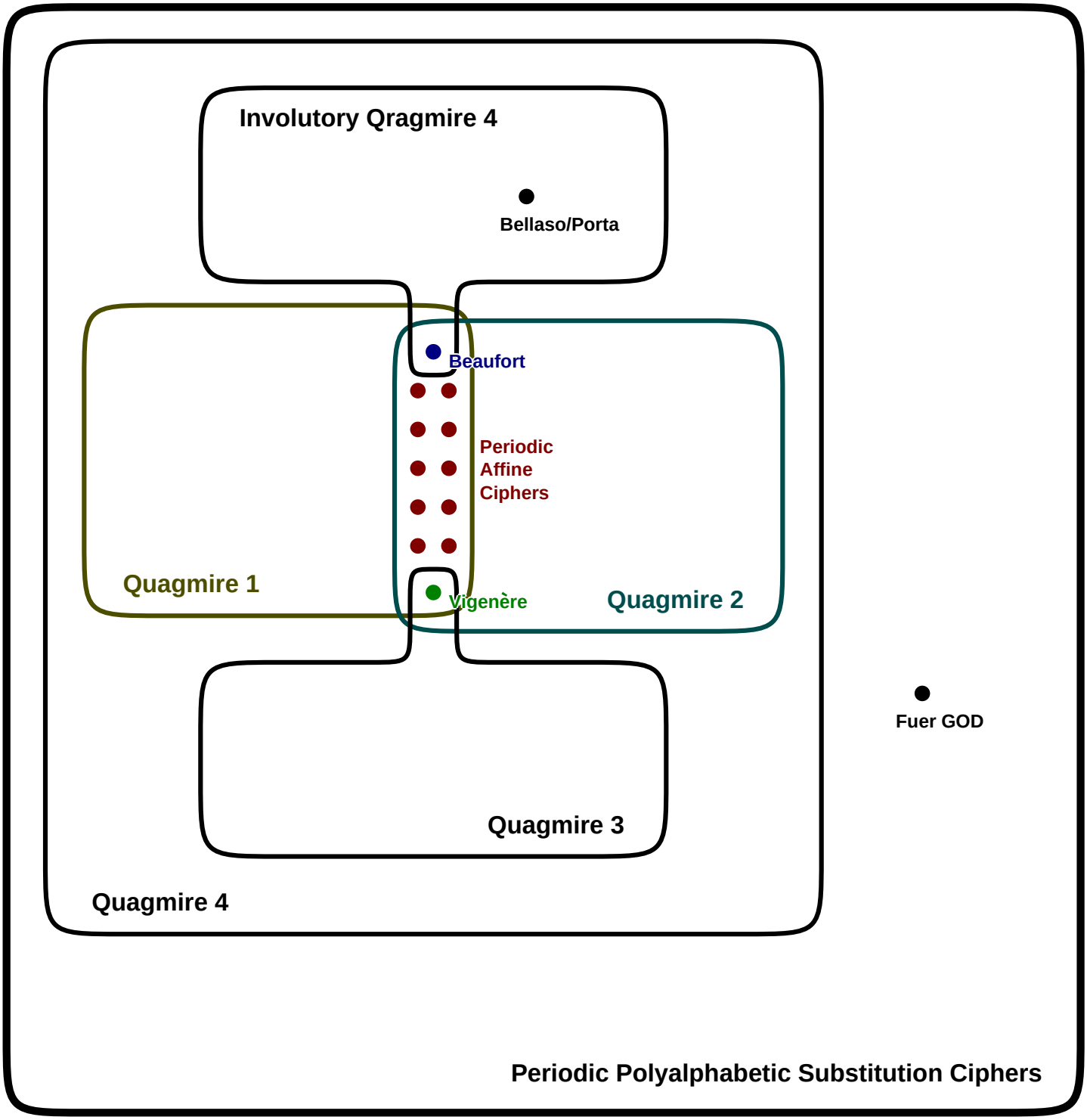
type 1: $k_n = b_n \circ k_{\text{base}}^{-1} = (R_{-n} \circ z) \circ k_{\text{base}}^{-1} = R_{-n} \circ (k_{\text{base}} \circ z)^{-1}$
type 2: $k_n = k_{\text{base}} \circ b_n = k_{\text{base}} \circ (z \circ R_n) = (k_{\text{base}} \circ z) \circ R_n$
type 3: $k_n = k_{\text{base}} \circ b_n \circ k_{\text{base}}^{-1} = k_{\text{base}} \circ (z \circ R_n) \circ k_{\text{base}}^{-1} = (k_{\text{base}} \circ z) \circ R_n \circ k_{\text{base}}^{-1}$
type 4: $k_n = k_C \circ b_n \circ k_P^{-1} = k_C \circ (z \circ R_n) \circ k_P^{-1} = (k_C \circ z) \circ R_n \circ k_P^{-1}$

We are unable to create a Q3 cipher in this way, but we see type 1 is Q1, type 2 is Q2, and types 3 and 4 are Q4.

That third category is somewhat interesting. They are isomorphs of B, and therefore also involutory, also called self-reciprocal. This gives us a prescription for creating a self-reciprocal Q4: Take any base key k_P and use its reversal as k_C. Furthermore, since $z \circ R_n = R_{-n} \circ z$, these quagmire 4s are left and right cosets of the *same* Q3, up to an automorphism that merely reorders the rows of its tableau. This last feature is shared by the Q4s that are isomorphs of any of the periodic affine ciphers, since $\{a_m \circ R_n\} = \{R_n \circ a_m\}$ for a given m. On the next page is a diagram summarizing our classification of quagmire ciphers.

Conclusion

We showed that the Beaufort cipher is simultaneously a quagmire 1 and a quagmire 2. Furthermore, it belongs to a family of periodic affine ciphers that share this property.


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

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; http://archive.org/details/cryptanalysis00gain.

[2] 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 https://www.cryptogram.org/downloads/aca.info/ciphers/Beaufort.pdf, QuagmireI.pdf, QuagmireII.pdf, QuagmireIII.pdf, QuagmireIV.pdf, and Vigenere.pdf.

[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.

[5] Thomas Kaeding, Quagmire ciphers and group theory: Recovering keywords from the key table, Cryptology ePrint Archive, report 2022/1475.

[6] For lack of a better reference, https://en.wikipedia.org/wiki/Atbash.