# A hexagonal Playfair cipher

Jimmy Mathews

January 2012

The standard Euclidean structure on the torus $S^1 \times S^1$, the one that descends from the usual metric on $\mathbf{R}^2$ to the quotient by the lattice generated by the two standard basis vectors, provides the setting for the classical Wheatstone-Playfair cipher. This article is about a variant of this cipher coming from a different choice, the Euclidean structure on the quotient of $\mathbf{R}^2$ by the lattice generated by the vectors $(1, 0)$ and $(\frac{1}{2}, \frac{\sqrt{3}}{2})$.

## The classical cipher

The Playfair cipher amounts to a map $c : C^2 \to C^2$ which encodes pairs of characters from a character set $C$ as other pairs. $|C|$ must be 1 greater than a composite number, so that all of the characters except one special character can be arranged on a rectangular grid. For example,

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

The rules for encoding a pair $(x, y)$ are the following:

- If $x$ and $y$ are on the same row, $c(x, y)$ is the shift of $x$ and $y$ one unit to the right. Letters with no right-side neighbor get rotated back to the beginning of the row.
- If $x$ and $y$ are on the same column, $c(x, y)$ is the shift of $x$ and $y$ one unit up. Letters with no neighbor above are rotated to the bottom.

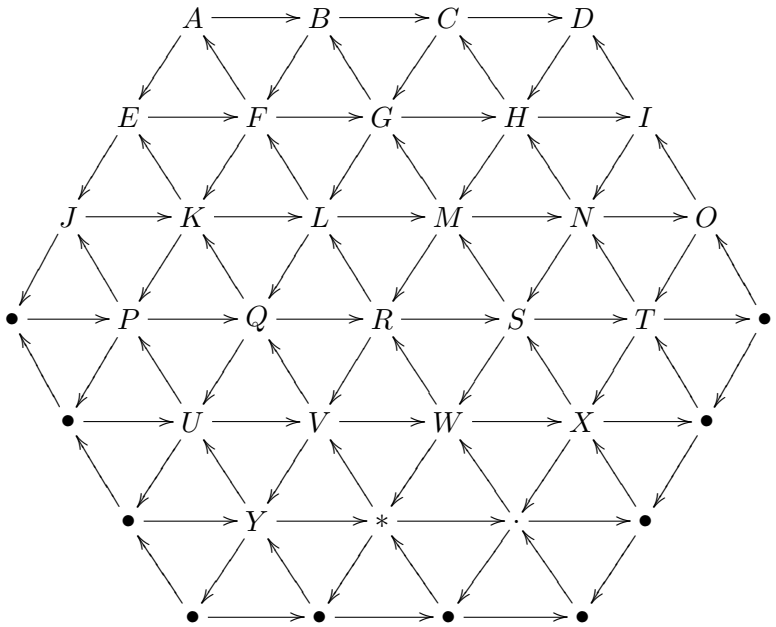
- If $x$ and $y$ are not on the same row or column, they are the corners of a unique rectangle. $c(x, y)$ is the pair consisting of the other corners, the one on the same row as $x$ appearing first.
- If $x = y$, $c(x, y)$ is $x$ and the special character (in the example, Z), in either order.
- If $x$ or $y$ is the special character, $c(x, y)$ is two of the other character.

Since the letters in the diagram can be arranged in any order agreed upon by the sender and the receiver, a person who doesn't know the arrangement would have a hard time guessing a message encoded with the cipher.

You might have guessed that the points of the key diagram are best understood as points on a torus. Let $e_1$ and $e_2$ be the standard basis of $\mathbf{R}^2$, and consider the torus given by the quotient of $\mathbf{R}^2$ by the lattice $\langle 5e_1, 5e_2\rangle$. The lattice points $L' = \langle e_1, e_2\rangle$ fall into 25 classes $L'/L$, corresponding to 25 points on the torus $\mathbf{R}^2/L$. Technically, the key data consists of a correspondence $L'/L \to C\backslash\{Z\}$, together with the specific choice $\{e_1, e_2\}$ of generators for $L'$ that tell us how to perform the shift operations. (Question: How many Euclidean symmetries of the torus preserve $L'/L$ and the set of distinguished directions $\{e_1, e_2\}$? How many keys are there (up to such symmetries)?)

## The hexagonal cipher

The variant will be a cipher $c : C^3 \to C^3$ that encodes triples of characters as other triples. Set $b_1 = e_1$, $b_2 = (\frac{1}{2}, \frac{\sqrt{3}}{2})$. Let $L = \langle 3(b_1 + b_2), 3(2b_2 - b_1)\rangle = \langle 3(b_1 + b_2), 9b_1\rangle$. The points of $L$ are the centers of a tiling of $\mathbf{R}^2$ by regular hexagons of side length 4. The points of the lattice $L' = \langle b_1, b_2\rangle$ are the vertices of a tiling of $\mathbf{R}^2$ by equilateral triangles of side length 1 subordinate to the hexagonal tiling. Note that $L'/L = \mathbf{Z}_3 \times \mathbf{Z}_9$ as abelian groups (in fact, for computer computations you probably want to work in this presentation of the group).



The key data will consist of:

- A special character $a \in C$
- A correspondence $L'/L \to C \setminus \{a\}$, where $|C| = 27 + 1$ (for example, $C$ is the usual alphabet with two additional characters like "space" and ".")
- A set of generators $p$,$q$, and $r$ for $L'$, each of length 1, satisfying $p + q + r = 0$ (for example, $\{b_1, b_2 - b_1, -b_2\}$ or $\{b_2, -b_1, b_1 - b_2\}$)
- An orientation on $\mathbf{R}^2/L$ (equivalent data is a cyclic ordering on $p$, $q$, and $r$)

The orbits in $L'/L$ of the actions of the elements of $\{p, q, r\}$ are called lines. The orbits of the actions of the elements of $\{p+q, q+r, r+p\}$ are called short lines. Lines are 9 units long, and short lines are 3 lattice units long (meaning, they contain 3 elements). There are 9 lines, in 3 parallel groups. There are 27 short lines, in 3 parallel groups. Each point belongs to 3 lines and 3 short lines.

The relevant group of symmetries is the group $G$ of Euclidean symmetries of the torus that preserve the lattice points. Such symmetries either preserve the actions of $\{p, q, r\}$ or reverse them. That is, the orientations on all of the lines is either preserved or reversed. The translation subgroup of $G$ is isomorphic to $L'/L$, while there is a rotation subgroup isomorphic to $D_{12}$. Since the translations have no fixed points, and all of the rotations do, these subgroups are disjoint. Moreover every element of $G$ can be written as a product, since a Euclidean symmetry is determined by where it sends a basepoint of $L'/L$ and the rotation about that point. So $G = D_{12} \ltimes L'/L$ has order $3^4 \cdot 2^4 = 324$.

If two points $x$,$y$ lie on exactly one line, the distance between them will be the smallest non-negative number $d$ such that $\pm(x - y) = dp$, $dq$, or $dr$. This $d$ can only be 0,1,2, or 4. If $x$ and $y$ lie on more than one line, they must lie on 3 lines, and the distance $d$ between them is 3. Moreover in this case there is exactly 1 other point in the intersection of these lines. Every point belongs to a unique triple with these properties. Also, if two points do not lie on a line, then they lie on a unique short line. There are 6 points not connected to a given $x$ by a line.

A different key with the same special character $a$ will be considered equivalent if there is some $g$ in $G$ relating the two correspondences $L'/L \to C \setminus \{a\}$, sending the line orientations to the new orientations, and sending the orientation to the new orientation. How many equivalence classes of such keys are there? Certainly $G$ acts on all keys (with their orientation data), and the classes are its orbits. There are $27! \cdot 2^2$ keys with orientation with a given $a$. Then there are $28 \cdot 27!/3^4 = 28 \cdot 26!/3$ actual keys.

The strategy will be to come up with a rule $c : C^3 \to C^3$ that commutes with $G$, so that it is well-defined on equivalent keys, but that commutes with as few other permutations as possible, so

that different keys don't produce the same cipher (which would increase the chances of guessing the cipher without needing the key!).

The cases for an ordered triple $(x, y, z)$ can be classified by the incidence data (the number of points lying on lines) and the distance between points.

It turns out that there are 18 congruence classes of configurations of 3 distinct points in the lattice. 13 of them have $S_3$ symmetry of the incidence data, of which 6 have $S_3$ symmetry of the distance data, 6 are triples that lie on a unique line, and the remaining configuration has distance data (1,2,4). 2 form acute angles in a minimal configuration, with distances (1,2,-) and (2,4,-). 2 form obtuse angles with distances (1,1,-), and (1,4,-). The last configuration has distance data (3,-,-).

For distinct $x$,$y$, $z$ all different from $a$, the rules are:

1. If all points lie on a unique line $l$, $c(x, y, z) = (t(x), t(y), t(z))$, where $t$ is the translation by one unit along the line hit first by an oriented rotation from $l$. Alternatively, you could translate along $l$, but then you might get some of the same letters in the encipherment.

2. The equilateral triangles of size 1, 2, and 4 come in concentric triples with one of each type. If the points form the vertices of a triangle of size 1, $c(x, y, z)$ is the sliding of these points (by 1 unit) along the sides of the associated triangle of size 2 to the vertices of this triangle. If of size 2, $c(x, y, z)$ is similar. If of size 4, $c(x, y, z)$ is a similar operation, sending each point 4 units along the line determined by the other two points, only in this geometry they end up as the points of the associated triangle of size 1.

3. Suppose $(x, y, z)$ form the vertices of an equilateral triangle of size 3. There are 6 possible centers, depending on the choice of representatives for the vertices. Of these, 3 are the centers of triangles whose order of vertices $x$, $y$, $z$ is positively oriented. Set $c(x, y, z)$ to be these 3 points, in an order so that $x$, $y$, $z$ are the centers of positively oriented triangles with these 3 points as vertices.

   Note that strictly speaking, $c$ restricted to the set of triples forming the vertices of size 3 equilateral triangles is only well-defined modulo the action of $\mathbf{Z}_3$ by order-preserving permutations on the domain $(x, y, z)$ and the range. This is acceptable because there are only 9 configurations where this rule is applied. It might seem that this operation groups the 9 sets of size 3 equilateral triples into pairs, an apparent contradiction. But it in fact pairs the 18 sets of such triples with orientation.

4. If no pair of points lies on a line, they must form either a short line or an equilateral triangle with short line sides. In the first case, set $c(x, y, z) = (t(x), t(y), t(z))$, where $t$ is translation by one unit along the line hit first by an oriented rotation from the short line. In the second case, there is a unique center. Set $c(x, y, z) = (R(x), R(y), R(z))$, where $R$ is the oriented rotation by $2\pi/6$ about this center.

5. If only one pair lies on a line $l$, their distance apart must be 3, and there is a minimal configuration in which the third point is one of the two closest lattice points to one of the $l$

along its perpendicular bisector. Set $c(x, y, z) = (t(x), t(y), t(z))$, where $t$ is the translation by one unit along the line hit first by an oriented rotation from $l$. Alternatively, one could choose $t$ to be the translation along $l$.

6. In every other case, there is a choice of representatives of $(x, y, z)$ so that they form consecutive vertices of a hexagon with possibly alternating side lengths. The other 3 vertices are unique. Set $c(x, y, z)$ to be these opposite vertices, in the same cyclic order.

For the case of repeated letters, or one of $x$,$y$,$z$ is the special character $a$:

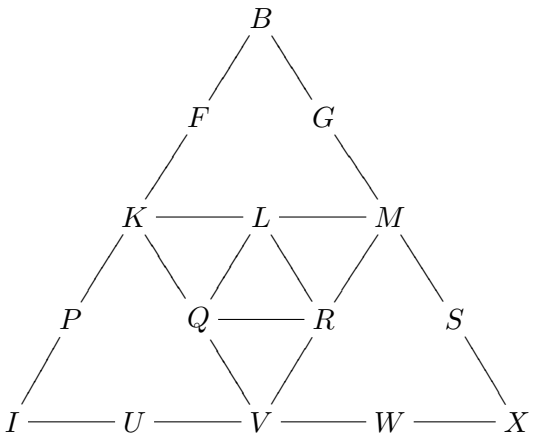
1. If there is a double letter $f \neq a$ and a single letter $g \neq a$, $c(x, y, z)$ has $a$ in the position of the single letter, followed by $t(f)$ and then $t(g)$ in cyclic order, where $t$ is the translation in the direction of the line first hit by an oriented rotation from the line through $f$ and $g$. (If there is more than one such line, we must simply permute $f$ and $g$).

2. If all are distinct but one of $x$, $y$, $z$ is $a$, let $f$ be the character before $a$ and let $g$ be the character after. $c(x, y, z)$ is $t(g)$ in the position of $a$, and $t(f)$ in the other two positions (where $t$ is as before).

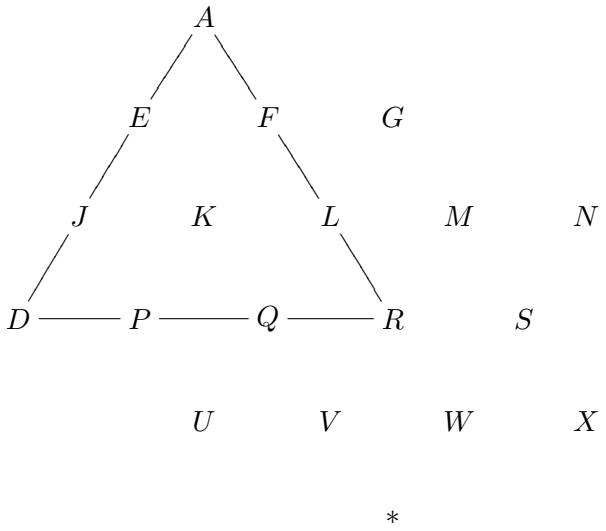
3. If there is a double letter $f \neq a$ and the third letter is $a$, $c(x, y, z)$ has an $f$ in the position of $a$ and two of $a$ in the other two positions.

4. If $a$ occurs as a double letter, and the third letter $f$ is not $a$, $c(x, y, z)$ has $a$ in the position of $f$ and two of $f$ in the other two positions.

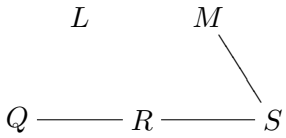
5. Triple letters are excluded from the domain, as the remaining choices would constitute a permutation of the character set (which would require about as much additional data as a new key).




$c(B, I, X) = (Q, R, L)$
$c(Q, R, L) = (K, V, M)$
$c(K, V, M) = (I, X, B)$




$c(A, D, R) = (K, *, N), (*, N, K), (N, K, *)$





$c(S, M, Q) = (W, L, V)$

## Strengthening the cipher

Given that the number of triples of characters is almost 22000, one way to strengthen the cipher considerably would be for the sender and receiver to maintain an ordered list of the 22000 most commonly used words. Then each word would stand for a triple (modulo the minor domain reductions indicated). That way if an attacker learns a correspondence between two triples, he only learns one word (not letters, which appear in many words).

One way to strengthen the cipher without having to maintain a long list of words is a dynamic key. For example, the special character could be swapped for the fulcrum node whenever the hexagon rule is applied, and the points lying on a line could be translated whenever a translation rule is applied. The receiver in possession of the initial key would have to start at the beginning of the message, decipher a triple, and then modify the key depending on the outcome. This would especially protect against frequency cryptanalysis.

As presented, the hexagonal Playfair cipher is very likely susceptible to known- and chosen-plaintext attacks.

## Symmetric key encryption

Despite the superiority (necessity?) of public key cryptography in terms of security over an insecure channel, symmetric key encryption systems are still widely used as the true medium of communication, the keys being exchanged via the more secure system. This is for performance; encrypting and decrypting all communication using RSA, for example, takes a long time. Encrypting just a key for a more elementary method is much easier.

The cipher is a symmetric key system with about 90-bit keys. For comparison, the Data Encryption Standard has 56-bit keys. Though the DES is now susceptible to a brute force attack, it was the system of choice for some decades until it was replaced ten years ago by the Advanced Encryption Standard, with 128-bit or 256-bit keys.