A Proposed Rubik's Cube Cipher vs. the Classic Trifid Cipher

Blake Willoughby
Arizona State University

Proposed Rubik's Cube Cipher.

Overview.

- Combination cipher - substitution, followed by transposition and fractionation.
- Key size - 21 permutations.
- Key space - $43,252,003,274,489,856,000 \cdot 5 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 5$.

Key Selection and Size.

A key is chosen by two parties, that is made up of, Φ, a composition of permutations of a $3 \times 3 \times 3$ Rubik's cube, R_3, and also a permutation $\tau \in S_3$, the group of all permutations of a 3 element set. Let $R_3 = \{F, B, R, L, U, D\}$ be the set of permutaions of a $3 \times 3 \times 3$ Rubik's cube, where each permutation is a 90 degree clockwise rotation of its repsective side.
We have $S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
All permutations of Rubik's cube can be reached in twenty moves or less, using the half-turn metric(Rokicki). Thus, the key size would be no greater than a composition of 20 permutations from the set R_3 and 1 non-identity permutation from the from the set S_3.

Keyspace.

There are 8 corner cubelets that can interchange with each other. There are 12 edges that can interchage with each other. Each corner can exist in three different states. Each edge can exist in two different states. Thus you would think the number of permutations is $(8!)(12!)(3^8)(2^{12})$. However, this counts the permutations of the faces twice, the orientations of the edges twice, and the orientations of the corners three times. Therefore, the total number of permutations of Rubik's cube is

$$\frac{(8!)(12!)(3^8)(2^{12})}{2 \cdot 2 \cdot 3} = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 \text{(Benton)}.$$

Then there are 5 different non-identity permutations in S_3.
Thus the keypace is $2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 5$.

Encryption.

Each side of Rubik's cube is assigned a permutation in S_3. In our example we have the following:

$$F = (1) \qquad R = (1\ 2) \qquad U = (1\ 2\ 3)$$
$$B = (1\ 3) \qquad L = (1\ 3\ 2) \qquad D = (2\ 3)$$

The key we have chosen in this example is the following:

$$Key: \Phi = U^2 D^2 R^2 L^2 F^2 B^2,\ \tau = (1\ 3\ 2)$$

Let us encrypt the plaintext "$Rubiks\ Cipher$."
We first permute Rubik's cube, by way of the composition Φ. Once permuted, we record the coordinates of each letter on their respective sides, and also record their permutation $\sigma_i \in S_3$ associated with the side the letter is on.

$Plaintext:$	R	u	b	i	k	s	C	i	p	h	e	r
x :	1	3	2	1	1	1	1	1	3	2	2	3
y :	3	3	1	3	2	3	1	3	1	3	2	3
$Side$:	L	D	D	U	L	D	F	U	R	D	U	R
σ_i :	(132)	(23)	(23)	(123)	(132)	(23)	(1)	(123)	(12)	(23)	(123)	(12)

We now recursively compute the premutation $\alpha_i \in S_3$ as follows:

$$\alpha_1 = \sigma_1 \circ \tau \text{ and } \alpha_{i+1} = \alpha_k \circ \sigma_{i+1}.$$

Finding the ciphertext, we have the following:

α_i :	(123)	(12)	(123)	(132)	(123)	(12)	(12)	(23)	(132)	(13)	(12)	(1)
$Side$:	U	R	U	L	U	R	R	D	L	B	R	F
$Ciphertext$:	1	L	t	p	x	J	P	a	l	T	N	C

Decryption.

For decryption you start with Rubik's cube in the standard orientation. Then record the coordinates of the letters in the ciphertext and the permutation associated with the side the letter is on. We then have the following:

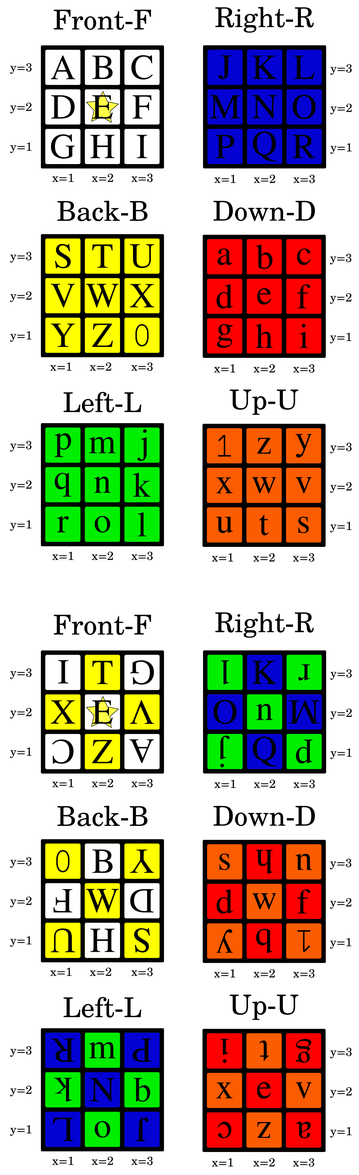
$Ciphertext$:	1	L	t	p	x	J	P	a	l	T	N	C
x :	1	3	2	1	1	1	1	1	3	2	2	3
y :	3	3	1	3	2	3	1	3	1	3	2	3
$Side$:	U	R	U	L	U	R	R	D	L	B	R	F
α_i	(123)	(12)	(123)	(132)	(123)	(12)	(12)	(23)	(132)	(13)	(12)	(1)

We now need to retrieve $\sigma_i \in S_3$, recursively, as follows:

$$\sigma_1 = \alpha_1 \circ \tau^{-1} \text{ and } \sigma_{i+1} = \alpha_i^{-1} \circ \alpha_{i+1}.$$

Permute Rubok's cube by way of Φ. Finding the plaintext, we have the following:

σ_i :	(132)	(23)	(23)	(123)	(132)	(23)	(1)	(123)	(12)	(23)	(123)	(12)
$Side$:	L	D	D	U	L	D	F	U	R	D	U	R
$Plaintext$:	R	u	b	i	k	s	C	i	p	h	e	r



Comparison.

Key Size.

- The key size of the Trifid Cipher is greater, but not by much.
- The key size of the proposed Rubik's Cipher can be shortened, in exchange for key space.

Keyspace.

- The key space of the Trifid Cipher is significantly greater.
- The key space of the Rubik's Cipher could be increased in exchange for a larger key size.

Security.

Both ciphers are susceptible to frequencey analysis and brute force prior to transposition and fractionation. However, the Rubik's cipher is less secure.

- To break the Rubik's Cipher, just try the 5 non-identity permutations in S_3.
- To break the Trifid Cipher, just try every number that divides the length of the message.

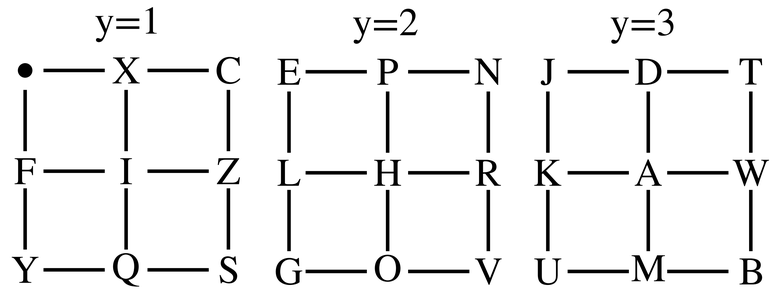
Trifid Cipher.

Overview.

- Combination cipher - substitution, followed by transposition and fractionation.
- Key size - 26 letters and 1 number.
- Key space - $403,291,461,126,605,635,584,000,000 = 26!$ and then some!!!

Key Selection and Size.

The key for the Trifid cipher is a $3 \times 3 \times 3$ array filled at random with the 26 letters of the alphabet. The last spot in the array is then filled with a dot. There is also an $n \in \mathbb{Z}_+$ that is chosen as the period that must divide the length of the message being sent.



Keyspace.

I can choose which letter goes in the first slot of the array 27 ways, 26 ways for the next slot, and so on, until I am out of letters. Thus, there are $27!$ ways to create the array. Then, how many numbers that divide the length of the message determines the total number of possible keys. Let l be how many numbers that will divide the length of the message. Then the keyspace is $27! \cdot l$.

Encryption.

Our key is the $3 \times 3 \times 3$ array seen in the picture. The period we have chosen is 4.
Let us encrypt the plaintext "$TRIFID\ CIPHER$."
We first record the coordinates associated with each letter in the key and then seperate the coordinate columns into groups of 4, the period, as follows:

$Plaintext:$	T	R	I	F	I	D	C	I	P	H	E	R
x :	3	3	2	1	2	2	3	2	2	2	1	3
y :	3	2	1	1	1	3	1	1	2	2	2	2
z :	3	2	2	2	2	3	3	2	3	2	3	2

We know concatenate the rows of each grouping as follows:

$$3\,3\,2\,1\,3\,2\,1\,1\,3\,2\,2\,2 \mid 2\,2\,3\,2\,1\,3\,1\,1\,2\,3\,3\,2 \mid 2\,2\,1\,3\,2\,2\,2\,2\,3\,2\,3\,2$$

We now start from the left and write these numbers in columns of 3 as follows:

x :	3	1	1	2	2	2	1	3	2	3	2	2
y :	3	3	1	2	2	1	1	3	2	2	2	3
z :	2	2	3	2	3	3	2	2	1	2	3	2
$Ciphertext$:	W	K	·	H	P	X	F	W	O	R	P	A

Decryption.

We use the same key for decryption as we used for encryption.
We start by recording the coordinates of the letters in the ciphertext:

$Ciphertext$:	W	K	·	H	P	X	F	W	O	R	P	A
x :	3	1	1	2	2	2	1	3	2	3	2	2
y :	3	3	1	2	2	1	1	3	2	2	2	3
z :	2	2	3	2	3	3	2	2	1	2	3	2

I then list the columns into one row and seperate it according to the period:

$$3\,3\,2\,1 \mid 3\,2\,1\,1 \mid 3\,2\,2\,2 \mid 2\,2\,3\,2 \mid 1\,3\,1\,1 \mid 2\,3\,3\,2 \mid 2\,2\,1\,3 \mid 2\,2\,2\,2 \mid 3\,2\,3\,2$$

We now stack every three groupings such that the first one is on top the second is in the middle and the third one is on the bottom. I then have the coordinates of the plaintext in columns:

x :	3	3	2	1	2	2	3	2	2	2	1	3
y :	3	2	1	1	1	3	1	1	2	2	2	2
z :	3	2	2	2	2	3	3	2	3	2	3	2
$Plaintext$:	T	R	I	F	I	D	C	I	P	H	E	R

Sources.

- Benton, Christopher. Counting the Number of Permutations in Rubik's Cube. Retrieved from http://docbenton.com/lecture-counting.pdf. Accessed: 11 November 2017.
- *Trifid Ciphers. Retrieved from https://math.asu.edu/sites/default/files/trifid.pdf. Accessed: 11 November 2017.*
- Rokicki, T., Kociemba, H., Davidson, M., and Dethridge, J. (2013). *The Diameter of the Rubik's Cube Group Is Twenty. SIAM Journal on Discrete Mathematics, 27(2), 1082-1105.*