8 Rearranging the Columns

The Problem

The formula for the disk cipher from Theorem 1 was $f_{\sigma,k} = f_\sigma \circ f_{\varepsilon,k'}$ where $k' = f_\sigma^{-1}(k)$. However we didn't use this formula in our analysis but rather a similar one of the type $f_{\sigma,k} = g \circ f_\sigma$ where g should describe the shifts in the alphabets and g^{-1} the rearrangement. What we did was first rearrange the shifts in the different columns, and then solve the resulting monoalphabetic ciphertext. Note that for this method to work in general the primary alphabet must be known. Unfortunately there is no useful general interpretation of the formula $g = f_\sigma \circ f_{\varepsilon,k'} \circ f_\sigma^{-1}$ when σ is unknown.

We'll analyze the situation, first for an example.

Example

We take the standard alphabet $\Sigma = \mathtt{A}\ldots\mathtt{Z}$, and consider an alphabet 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
---------------------------------------------------
Q W E R T Z U I O P A S D F G H J K L Y X C V B N M
W E R T Z U I O P A S D F G H J K L Y X C V B N M Q
E R T Z U I O P A S D F G H J K L Y X C V B N M Q W
...                         ...                 ...
M Q W E R T Z U I O P A S D F G H J K L Y X C V B N
```

Phrased in terms of permutations the top row, Row 0, the standard alphabet, corresponds to the identical permutation $\varepsilon \in \mathcal{S}(\Sigma)$. The next row, Row 1, the primary alphabet, corresponds to the permutation $\sigma \in \mathcal{S}(\Sigma)$. Row 2 corresponds to $\sigma \circ \tau$, where τ is the alphabet shift

$$\tau(\mathtt{A}) = \mathtt{B}, \quad \tau(\mathtt{B}) = \mathtt{C}, \quad \ldots, \quad \tau(\mathtt{Z}) = \mathtt{A}$$

Row i corresponds to $\sigma \circ \tau^{i-1}$. For the concrete example we have

$$\sigma(\mathtt{A}) = \mathtt{Q}, \quad \sigma(\mathtt{B}) = \mathtt{W}, \quad \ldots$$

and thus

$$\sigma \circ \tau(\mathtt{A}) = \sigma(\mathtt{B}) = \mathtt{W}, \quad \sigma \circ \tau(\mathtt{B}) = \sigma(\mathtt{C}) = \mathtt{E}, \quad \ldots$$

On the other hand

$$\tau \circ \sigma(\mathtt{A}) = \tau(\mathtt{Q}) = \mathtt{R}, \quad \tau \circ \sigma(\mathtt{B}) = \tau(\mathtt{W}) = \mathtt{X}, \quad \ldots$$

Shifts in the Primary Alphabet

Recall the alphabet table in the general case

s_0	s_1	s_2	$\ldots$	s_{n-1}
t_0	t_1	t_2	$\ldots$	t_{n-1}
t_1	t_2	t_3	$\ldots$	t_0
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
t_{n-1}	t_0	t_1	$\ldots$	t_{n-2}

where $t_i = \sigma s_i$ for $0 \leq i \leq n-1$, and σ is the permutation that defines the primary alphabet.

Identify as usual the alphabet $\Sigma = \{s_0, \ldots, s_{n-1}\}$ with $\mathbb{Z}/n\mathbb{Z}$, the integers $\bmod n$, via $i \mapsto \sigma_i$ and take indices $\bmod n$. Mathematical expressions for the shifts in the original and primary alphabets are

- $\tau =$ shift by 1 in the original alphabet, $\tau(s_i) = s_{i+1}$.
- $\tau^k =$ shift by k in the original alphabet, $\tau^k(s_i) = s_{i+k}$.
- $\sigma\tau\sigma^{-1} =$ shift by 1 in the primary alphabet,

$$t_i \overset{\sigma^{-1}}{\mapsto} s_i \overset{\tau}{\mapsto} s_{i+1} \overset{\sigma}{\mapsto} t_{i+1}$$

- $\sigma\tau^k\sigma^{-1} = (\sigma\tau\sigma^{-1})^k =$ shift by k in the primary alphabet.

The alphabet table, interpreted as list of permutations, is the orbit of $\sigma \in \mathcal{S}(\Sigma)$ under iterated right translation by τ (or under the cyclic subgroup $\langle\tau\rangle \subseteq \mathcal{S}(\Sigma)$ generated by τ).

The "naive" shift that we performed in Section 7 shifted the single letters of the primary alphabet by a certain number of positions in the *standard* alphabet—we performed $\tau^i \circ \sigma$ for some value i. Why was this successful? Under what conditions are the naively shifted primary alphabets again rows of the alphabet table?

Decimated alphabets

We take the ordering of the alphabets into account and let $T_1 = (t_0, \ldots, t_{n-1})$ be the ordered primary alphabet where $t_i = \sigma s_i$. The secondary alphabets then are $T_i = (t_{i-1}, \ldots, t_{n-1}, t_0, \ldots, t_{i-2})$ for $i = 2, \ldots, n$. They correspond to the permutations $\sigma \circ \tau^{i-1}$, that is $T_i = (\sigma s_{i-1}, \sigma s_i, \ldots)$.

The primary alphabet used in the example of Section 7 was of a special kind: It had $t_i = s_{3i \bmod 26}$. The corresponding formula for the general case is

$$t_i = s_{ki \bmod n},$$

and t_i for $i = 0, \ldots, n-1$ runs through all elements of Σ if and only if k and n are relative prime.

Definition. Let the alphabet Σ be linearly ordered as $(s_0, \ldots, s_{n-1})$, and let $\gcd(k, n) = 1$. The (ordered) alphabet $T = (t_0, \ldots, t_{n-1})$ is called **decimated alphabet** of order k (of Σ with the given linear order relation) if there is an index $p \in \{0, \ldots, n-1\}$ such that $t_{p+i} = s_{ki \bmod n}$ for $i = 0, \ldots, n-1$.

That means, beginning with $t_p = s_0$ we take each k-th letter from Σ.

If the primary alphabet is decimated, so are all the secondary alphabets; we get them all by varying the index p.

Now when we apply the shift τ to the (ordered) primary and secondary alphabets $T_1, \ldots, T_n$ we get new alphabets $f_\tau(T_1), \ldots, f_\tau(T_n)$; note that we interpret the n-tuples T_i as texts and apply τ elementwise. The question we want to answer is whether the $f_\tau(T_i)$ belong to the collection of the T_i. The answer involves the normalizer $N(\langle\tau\rangle)$ of the subgroup $\langle\tau\rangle \leq \mathcal{S}(\Sigma)$.

Theorem 2 (Decimated alphabets) *Let the alphabet Σ be linearly ordered as $(s_0, \ldots, s_{n-1})$. Let the (ordered) primary alphabet $T_1 = (t_0, \ldots, t_{n-1})$ be defined by $t_i = \sigma s_i$ where $\sigma \in \mathcal{S}(\Sigma)$, and let $T_2, \ldots, T_n$ be the corresponding ordered secondary alphabets. Then the following statements are equivalent:*

(i) *There is a $j \in \{1, \ldots, n\}$ with $f_\tau(T_1) = T_j$.*

(ii) *f_τ permutes the $\{T_1, \ldots, T_n\}$.*

(iii) *T_1 is a decimated alphabet of Σ.*

(iv) *$\sigma \in N(\langle\tau\rangle)$.*

Proof. "(i) $\Longrightarrow$ (iv)": $f_\tau(T_1) = T_j$ means that $\tau \circ \sigma = \sigma \circ \tau^j$. Then $\sigma^{-1} \circ \tau \circ \sigma \in \langle\tau\rangle$ or $\sigma \in N(\langle\tau\rangle)$.

"(iv) $\Longrightarrow$ (iii)": By conjugation σ defines an automorphism of the cyclic group $\langle\tau\rangle$. These automorphisms are known, the following Lemma 1 gives $\sigma \circ \tau \circ \sigma^{-1} = \tau^k$ for some k, relative prime with n. The letter s_0 occurs somewhere in T_1, so let $s_0 = t_p$. Then $\sigma s_p = t_p = s_0$ and

$$t_{j+p} = \sigma s_{j+p} = \sigma\tau^j s_p = \tau^{jk}(\sigma s_p) = \tau^{jk} s_0 = s_{jk} \quad \text{for } j = 0, \ldots, n-1,$$

where as usual we take the indices $\bmod\, n$.

"(iii) $\Longrightarrow$ (iv)": Let p and k as in the definition. For any i we have

$$\tau^k \sigma s_{p+i} = \tau^k t_{p+i} = \tau^k s_{ki} = s_{ki+k} = s_{k(i+1)} = t_{p+i+1} = \sigma s_{p+i+1} = \sigma\tau s_{p+i}.$$

From this we conclude $\sigma \circ \tau = \tau^k \circ \sigma$ or $\sigma \circ \tau \circ \sigma^{-1} \in \langle\tau\rangle$.

"(iv) $\Longrightarrow$ (ii)": We have $\sigma^{-1} \circ \tau \circ \sigma = \tau^{k'}$ where $k'k \equiv 1 \pmod{n}$ whence $\tau \circ \sigma = \sigma \circ \tau^{k'}$. The permuted alphabet T_i corresponds to the permutation $\sigma \circ \tau^{i-1}$. Therefore $f_\tau T_i$ corresponds to $\tau \circ \sigma \circ \tau^{i-1} = \sigma \circ \tau^{k'+i-1}$. We conclude $f_\tau T_i = T_{k'+i}$.

"(ii) $\Longrightarrow$ (i)" is the restriction to a special case. ◇

Lemma 1 *Let $G = \langle g \rangle$ be a finite cyclic group of order m. Then the automorphisms of G are the power maps $g \mapsto g^k$ where k is relatively prime to m. In other words, the automorphism group* $\operatorname{Aut} G$ *is isomorphic with the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. Let h be an automorphism of G. Then $h(g) = g^k$ for some $k \in \mathbb{Z}$. This k uniquely defines h on all of G, and k is uniquely determined by h up to multiples of $\operatorname{Ord}(g) = m$. The power map $g \mapsto g^k$ is bijective if and only if k is relatively prime to m. $\diamond$