2 Examples of Multiple Ciphers

Examples of Groups

Each of the following length preserving ciphers forms a group:

- The shift ciphers over Σ with respect to a group structure on Σ
- The monoalphabetic substitutions over Σ
- The Bellaso ciphers with a fixed period
- The block transpositions of a fixed length

DES

DES is a block cipher on $\mathbb{F}_2^{64}$ with keyspace $\mathbb{F}_2^{56}$. Campbell and Wiener in (Crypto 92) proved that DES generates the alternating group of order 2^{64}. Shortly before Coppersmith had shown that the group order is at least 10^{277}. Only much later someone noted that Moore and Simmons in Crypto 86 had published the lengths of several cycles that would have sufficed to show that DES is not a group—a fact that for several years was viewed as an open conjecture.

Historical Examples

The composition of a polyalphabetic cipher of period l and another one of period q has period $\mathrm{lcm}(l, q)$. **Application:** Key generating machines as mentioned in Part I, see the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/4_Cylinder/LongPeriods.html`.

Another historical example: the double columnar transposition that is considerably stronger than the simple columnar transposition.

Composition of Bellaso Cipher

The composition of two Bellaso ciphers of periods l and q has period $\mathrm{lcm}(l, q)$, essentially the product lq. However its security amounts at most to the sum $l + q$ in view of an attack with known plaintext:

Assume known plaintext of length $l + q$ (over the alphabet $\mathbb{Z}/n\mathbb{Z}$). This yields $l + q$ linear equations for $l + q$ unknows—the characters of the two keys. Assume that $l < q$. Then the situation is

Plaintext	a_0	a_1	$\dots$	a_{l-1}	a_l	$\dots$	a_{q-1}	$\dots$
Key 1	h_0	h_1	$\dots$	h_{l-1}	h_0	$\dots$	$\dots$	$\dots$
Key 2	k_0	k_1	$\dots$	k_{l-1}	k_l	$\dots$	k_{q-1}	$\dots$
Ciphertext	c_0	c_1	$\dots$	c_{l-1}	c_l	$\dots$	c_{q-1}	$\dots$

Taken together this is a BELLASO cipher with key

$$(h_0 + k_0, h_1 + k_1, \ldots)$$

and period $\operatorname{lcm}(l, q)$.

Let the known plaintext be $(a_0, \ldots, a_{l+q-1})$. Then the system of linear equations for the $l + q$ unknowns $h_0, \ldots, h_{l-1}, k_0, \ldots, k_{q-1} \in \mathbb{Z}/n\mathbb{Z}$ is:

$$\begin{aligned}
h_0 + k_0 &= c_0 - a_0,\\
h_1 + k_1 &= c_1 - a_1,\\
&\vdots\\
h_{l-1} + k_{l-1} &= c_{l-1} - a_{l-1},\\
h_0 + k_l &= c_l - a_l,\\
&\vdots\\
h_{l+q-1 \bmod l} + k_{l+q-1 \bmod q} &= c_{l+q-1} - a_{l+q-1}.
\end{aligned}$$

This cannot have a unique solution: If we add a fixed value x to all h_i, and subtract x from all k_j, then we get another solution. Therefore for simplicity we may assume $h_0 = 0$. If the keys are not randomly chosen but built from keywords, then a simple "CAESAR exhaustion" will reveal the "true" keys later. For decryption the shifted keys are equivalent. And since we eliminated one unknown quantity, in general even $l + q - 1$ known plaintext letters are enough for uniquely solving the remaining $l + q - 1$ equations. We won't go into the details but give an exercise for interested readers.

Exercise

Consider the ciphertext

```
CIFRX KSYCI IDJZP TINUV GGKBD CWWBF CGWBC UXSNJ LJFMC
LQAZV TRLFK CPGYK MRUHO UZCIM NEOPP LK
```

For an attack with known plaintext assume that

- the plaintext (is in German and) starts with "Sehr geehrter ..." (a common beginning of a letter)
- some keylengths are already ruled out by trial & error; the actual lengths to test for a double BELASO cipher are $42 = 6 \times 7$.

(A coincidence analysis, even if it doesn't give enough confidence in a definite period, should suffice to exclude all but a few combinations of possible keylengths.)