5 Cryptanalysis of the Linear Cipher

Block Length

The block length l leaves its trace as a divisor of the ciphertext length. If however the sender conceals the procedure by padding with meaningless text the cryptanalyst has no choice than to try all possible lengths by brute force.

Known Plaintext

Cryptanalyzing the linear cipher needs known plaintext—or some probable plaintext and a bit of trial and error to find the correct position. If the cryptanalyst knows the block length l and has l blocks of known plaintext she only has to solve a system of linear equations. This amounts to known plaintext of l^2 letters, corresponding to the length of the key. In a few degenerate cases she needs some additional known plaintext.

Let $(a_{11}, \ldots, a_{l1}), \ldots, (a_{1l}, \ldots, a_{ll})$ be the blocks of known plaintext, not necessarily contiguous, and $(c_{11}, \ldots, c_{l1}), \ldots, (c_{1l}, \ldots, c_{ll})$, the corresponding ciphertext blocks.

This yields the matrix equation

$$\begin{pmatrix} k_{11} & \ldots & k_{1l} \\ \vdots & \ddots & \vdots \\ k_{l1} & \ldots & k_{ll} \end{pmatrix} \begin{pmatrix} a_{11} & \ldots & a_{1l} \\ \vdots & \ddots & \vdots \\ a_{l1} & \ldots & a_{ll} \end{pmatrix} = \begin{pmatrix} c_{11} & \ldots & c_{1l} \\ \vdots & \ddots & \vdots \\ c_{l1} & \ldots & c_{ll} \end{pmatrix},$$

in short: $kA = C$ in $M_{ll}(\mathbb{Z}/n\mathbb{Z})$. Note that the lowercase letter k also denotes an $l \times l$-matrix. In the lucky (but common) case where A is invertible we immediately solve for k and get the key

$$k = CA^{-1}.$$

Inverting a matrix is efficient by Section 2. Furthermore with high probability A is invertible, see Section 4. Otherwise the cryptanalyst needs some more plaintext. Instead of explicating the solution in detail we consider an example.

Example

Imagine the example of Section 3 is part of a longer text, and the plaintext `Herr` is known as well as its location. It consists of two blocks and defines the matrix

$$A = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

The determinant is $\operatorname{Det} A = 17 \cdot (7 \cdot 1 - 4 \cdot 1) = 17 \cdot 3 = 51 \equiv -1 \bmod 26$. The cryptanalyst has luck. She immediately calculates the inverse:

$$A^{-1} = \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix}.$$

From this she gets the key matrix:

$$k = \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} \begin{pmatrix} 9 & 17 \\ 4 & 19 \end{pmatrix} = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Solving the Affine Cipher

For solving the affine cipher $c = ka + b$ the cryptanalyst in general needs $l + 1$ blocks of known plaintext $a_0, \ldots, a_l$. By forming differences she gets

$$\begin{aligned} c_l - c_0 &= k \cdot (a_l - a_0), \\ &\ldots \\ c_l - c_{l-1} &= k \cdot (a_l - a_{l-1}). \end{aligned}$$

This reduces the cryptanalysis to that of the linear cipher with l known plaintext blocks.

Summary

Linearity makes a cipher extremely vulnerable for a known plaintext attack. The reason is that systems of linear equations are easily solved, at least over rings that allow practical calculations. (This however is a basic prerequisite for a ring to be useful for cryptography.)

In constructing secure ciphers on wants to prevent known plaintext attacks. Therefore one has to bring in nonlinearity: Solving algebraic equation of higher degree is much more complex. Hence the memento:

Known plaintext is adversary to linearity.

Exercise. HILL's proposal comprised a permutation of the alphabet before applying the linear map. That means executing a monoalphabetic substitution first. Explore the effect on cryptanalysis.