3 The Linear Cipher

Description

The **alphabet** is $\Sigma = \mathbb{Z}/n\mathbb{Z}$ with the structure as a finite ring.

The **keyspace** is $K = GL_l(\mathbb{Z}/n\mathbb{Z})$, the multiplicative group of invertible matrices. Section 4 estimates the size of the keyspace.

We **encrypt** blockwise taking blocks of length l: For $k \in GL_l(\mathbb{Z}/n\mathbb{Z})$ and $(a_1, \ldots, a_l) \in (\mathbb{Z}/n\mathbb{Z})^l$ set

$$\begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix} = f_k(a_1, \ldots, a_l) = k \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix}$$

or elementwise

$$c_i = \sum_{j=1}^{l} k_{ij} a_j \quad \text{for } i = 1, \ldots, l.$$

We **decrypt** with the inverse matrix:

$$\begin{pmatrix} a_1 \\ \vdots \\ a_l \end{pmatrix} = k^{-1} \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_l \end{pmatrix}.$$

Related Ciphers

Special case: Taking k as permutation matrix P_σ for a permutation $\sigma \in \mathcal{S}_l$ the encryption function f_k is the block transposition defined by σ.

Generalization: The affine cipher. Choose as key a pair

$$(k, b) \in GL_l(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^l.$$

Encrypt by the formula

$$c = ka + b.$$

Choosing the unit matrix for k (as special case) gives the Bellaso cipher with key b.

Remark The original cipher proposed by Hill first permuted the alphabet before applying the linear map. The correspondence between the letters and the numbers $0, \ldots, 25$ is treated as part of the key.

Example

As an illustration we take a "toy example" of unreasonable small dimension $l = 2$ and

$$k = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}.$$

Then $\operatorname{Det} k = 77 - 24 = 53 \equiv 1 \bmod 26$ and

$$k^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

The table

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

gives the correspondence between letters and numbers.

Now the plaintext `Herr` $= (7, 4, 17, 17)$ is encrypted as

$$\begin{aligned} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 \\ 4 \end{pmatrix} &= \begin{pmatrix} 77+32 \\ 21+28 \end{pmatrix} = \begin{pmatrix} 109 \\ 49 \end{pmatrix} = \begin{pmatrix} 5 \\ 23 \end{pmatrix}, \\ \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 17 \\ 17 \end{pmatrix} &= \begin{pmatrix} 187+136 \\ 51+119 \end{pmatrix} = \begin{pmatrix} 323 \\ 170 \end{pmatrix} = \begin{pmatrix} 11 \\ 14 \end{pmatrix}. \end{aligned}$$

Thus $f_k(\texttt{Herr}) = (5, 23, 11, 14) = \texttt{FXLO}$.

We verify this by decrypting:

$$\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 5 & 11 \\ 23 & 14 \end{pmatrix} = \begin{pmatrix} 35+414 & 77+252 \\ 115+253 & 253+154 \end{pmatrix} = \begin{pmatrix} 7 & 17 \\ 4 & 17 \end{pmatrix}.$$

Assessment

+ The linear cipher is stronger than block transposition and Bellaso cipher.

+ The frequency distribution of the ciphertext letters is nearly uniform. An attack with ciphertext only doesn't find useful clues.

− The linear cipher is extremely vulnerable for an attack with known plaintext, see Section 5.