8 The Similarity of Columnar and Block Transpositions

See the web page `http://www.staff.uni-mainz.de/pommeren/Cryptology/Classic/8_Transpos/Similar.html`

Permutation Matrices

Let $\sigma \in \mathcal{S}_p$ be a permutation of the numbers $1, \ldots, p$.

Let R be a ring (commutative with 1). Then σ acts on R^p, the free R-module with basis

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \ldots, \quad e_p = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix},$$

as the linear automorphism

$$\rho(\sigma) \quad \text{defined by} \quad \rho(\sigma)e_i = e_{\sigma i}.$$

This gives an injective group homomorphism

$$\rho\colon \mathcal{S}_p \longrightarrow GL(R^p).$$

How to express $\rho(\sigma)$ as a matrix? The vector

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = x_1 e_1 + \cdots + x_p e_p$$

maps to

$$\rho(\sigma)x = x_1 e_{\sigma 1} + \cdots + x_p e_{\sigma p} = \begin{pmatrix} x_{\sigma^{-1}1} \\ \vdots \\ x_{\sigma^{-1}p} \end{pmatrix}.$$

Thus the matrix P_σ corresponding to $\rho(\sigma)$ is given by

$$P_\sigma \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}1} \\ \vdots \\ x_{\sigma^{-1}p} \end{pmatrix} \quad \text{for all } x \in R^p.$$

Therefore

$$P_\sigma = (a_{ij})_{1 \le i,j \le p} \quad \text{where} \quad a_{ij} = \begin{cases} 1, & \text{if } i = \sigma j, \\ 0 & \text{otherwise.} \end{cases}$$

Hence the matrix P_σ has exactly one 1 in each row and in each column, all other entries being 0. We call P_σ the **permutation matrix** belonging to σ.

Matrix Description of a Block Transposition

The permutation σ defines a block transposition f_σ over the alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$: For $(a_1, \ldots, a_p) \in \Sigma^p$ let

$$f_\sigma(a_1, \ldots, a_p) = \left[P_\sigma \begin{pmatrix} a_1 \\ \vdots \\ a_p \end{pmatrix} \right]^T = (a_{\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}).$$

This moves the i-th letter a_i of the block to position σi.

More generally let $r = pq$ and $a = (a_1, \ldots, a_r) \in \Sigma^r$. Then

$$c = f_\sigma(a) = (a_{\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}, a_{p+\sigma^{-1}1}, \ldots, a_{p+\sigma^{-1}p}, \ldots, a_{(q-1)p+\sigma^{-1}p}).$$

From this we derive the general encryption formula:

$$c_{i+(j-1)p} = a_{\sigma^{-1}i+(j-1)p} \quad \text{for } 1 \le i \le p, 1 \le j \le q.$$

We may express this in matrix notation writing the plaintext as a matrix with $a_{i+(j-1)p}$ in row i and column j:

$$A = \begin{pmatrix} a_1 & a_{p+1} & \cdots & a_{(q-1)p+1} \\ \vdots & \vdots & a_{i+(j-1)p} & \vdots \\ a_p & a_{2p} & \cdots & a_{qp} \end{pmatrix} \in M_{p,q}(\mathbb{Z}/n\mathbb{Z}).$$

Analogously we write the ciphertext as $C \in M_{p,q}(\mathbb{Z}/n\mathbb{Z})$ where $C_{ij} = c_{i+(j-1)p}$ for $1 \le i \le p$, $1 \le j \le q$.

Then the encryption formula simply is the matrix product:

$$C = P_\sigma A$$

with the permutation matrix P_σ.

Matrix Description of a Columnar Transposition

The permutation σ also defines a columnar transposition g_σ over the alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$: Writing the plaintext row by row in a $q \times p$-matrix gives just the transposed matrix A^T (again assume $r = pq$):

$$\begin{array}{cccccccc} & & & & & \downarrow & & \downarrow \\ \rightarrow & a_1 & \cdots & a_p & & a_{\sigma^{-1}1} & \cdots & a_{\sigma^{-1}p} \\ \rightarrow & a_{p+1} & \cdots & a_{2p} & \mapsto & a_{p+\sigma^{-1}1} & \cdots & a_{p+\sigma^{-1}p} \\ & \vdots & a_{(\mu-1)p+\nu} & \vdots & & \vdots & a_{(\mu-1)p+\sigma^{-1}\nu} & \vdots \\ \rightarrow & a_{(q-1)p+1} & \cdots & a_{qp} & & a_{(q-1)p+\sigma^{-1}1} & \cdots & a_{(q-1)p+\sigma^{-1}p} \end{array}$$

and the ciphertext is read off, as the little arrows suggest, column by column in the order given by σ. Thus the encryption function is given by:

$$\tilde{c} = g_\sigma(a_1, \ldots a_r) = (a_{\sigma^{-1}1}, a_{p+\sigma^{-1}1}, \ldots, a_{\sigma^{-1}p}, \ldots, a_{(q-1)p+\sigma^{-1}p}).$$

The encryption formula is:

$$\begin{aligned} \tilde{c}_{\mu+(\nu-1)q} &= a_{(\mu-1)p+\sigma^{-1}\nu} \quad \text{for } 1 \leq \mu \leq q, 1 \leq \nu \leq p \\ &= c_{\nu+(\mu-1)p}. \end{aligned}$$

If we arrange $\tilde{c}$ column by column as a matrix

$$\tilde{C} = \begin{pmatrix} \tilde{c}_1 & \tilde{c}_{q+1} & \cdots & \tilde{c}_{(p-1)q+1} \\ \vdots & \vdots & \tilde{c}_{\mu+(\nu-1)q} & \vdots \\ \tilde{c}_q & \tilde{c}_{2q} & \cdots & \tilde{c}_{pq} \end{pmatrix} \in M_{q,p}(\mathbb{Z}/n\mathbb{Z}),$$

we see that

$$\tilde{C}^T = C = P_\sigma A.$$

This shows:

Proposition 1 *The result of the columnar transposition corresponding to $\sigma \in \mathcal{S}_p$ on Σ^{pq} arises from the result of the block transposition corresponding to σ by writing the latter ciphertext in p rows of width q and transposing the resulting matrix. This produces the former ciphertext in q rows of width p.*

In particular columnar transposition and block transposition are similar.

(The proposition describes the required bijection of Σ^* for strings of length pq.)

For texts of a length not a multiple of p this observation applies after padding up to the next multiple of p. For a columnar transposition with an uncompletely filled last row this does not apply. In spite of this we assess columnar and block transpositions as similar, and conclude: Although a columnar transposition permutes the text over its complete length without period, and therefore seems to be more secure at first sight, it turns out to be an *illusory complication*.