Ähnlichkeit zwischen Spalten- und Blocktranspositionen[1]

Sei $\sigma \in \mathcal{S}_p$ eine Permutation der Zahlen $1, \ldots, p$.

Permutationsmatrizen

Sei R ein Ring. Dann definiert σ auf R^p, dem freien R-Modul mit Basis

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

den linearen Automorphismus

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

Dadurch ist ein injektiver Gruppenhomomorphismus

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

gegeben.

Wie drückt sich $\rho(\sigma)$ durch eine Matrix aus? Der Vektor

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

wird abgebildet auf

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

Also ist die zu $\rho(\sigma)$ gehörige Matrix P_σ gegeben durch

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

Also ist

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

Die MatrixP_σ hat also in jeder Zeile und Spalte genau eine 1 und sonst nur Nullen und heißt die zu σ gehörige **Permutationsmatrix**.

[1] Klaus Pommerening, Kryptologie; 20. Juni 2002, letzte Änderung: 23. Januar 2008

Matrix-Beschreibung einer Blocktransposition

Die Permutation σ definiert über dem Alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$ eine Blocktransposition f_σ: Für $(a_1, \ldots, a_p) \in \Sigma^p$ ist

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

D. h., der i-te Buchstabe a_i des Blocks wird an die Stelle σi verschoben.

Allgemeiner sei $r = pq$ und $a = (a_1, \ldots, a_r) \in \Sigma^r$. Dann ist

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

Also ist die allgemeine Formel für die Verschlüsselung:

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

Dies lässt sich auch im Matrix-Schreibweise ausdrücken mit $a_{i+(j-1)p}$ in Zeile i und Spalte j; der Klartext wird also geschrieben als:

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

Der Geheimtext wird analog als $C \in M_{p,q}(\mathbb{Z}/n\mathbb{Z})$ geschrieben mit $C_{ij} = c_{i+(j-1)p}$ für $1 \le i \le p$, $1 \le j \le q$.

Dann ist die Verschlüsselungsformel gerade das Matrizen-Produkt:

$$C = P_\sigma A$$

mit der Permutationsmatrix P_σ.

Matrix-Beschreibung einer Spaltentransposition

Die Permutation σ definiert über dem Alphabet $\Sigma = \mathbb{Z}/n\mathbb{Z}$ auch eine Spaltentransposition g_σ: Der Klartext wird zeilenweise in eine $q \times p$-Matrix geschrieben, die gerade die Transponierte A^T ist (wieder wird $r = pq$ angenommen):

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

und der Geheimtext wird, wie angedeutet, spaltenweise in der durch σ vorgegebenen Reihenfolge ausgelesen; zeilenweise geschrieben sieht die Verschlüsselungsfunktion also so aus:

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

Also ist die Formel für die Verschlüsselung:

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

Schreibt man $\tilde{c}$ wieder spaltenweise in eine Matrix

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

so sieht man

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

Damit ist gezeigt:

Satz 1 *Das Ergebnis der Spaltentransposition zu $\sigma \in \mathcal{S}_p$ auf Σ^{pq} geht aus dem Ergebnis der Blocktransformation zu σ dadurch hervor, dass der letztere Geheimtext in p Zeilen der Breite q aufgeschrieben und die dadurch entstandene Matrix transponiert wird; es entsteht der erstere Geheimtext in q Zeilen der Breite p.*

Insbesondere sind Spalten- und Blocktransposition ähnlich.

(Die Bijektion von Σ^* wird auf Zeichenketten der Länge pq gerade so beschrieben wie im Satz.)

Für Texte der Länge, die nicht Vielfaches von p ist, gilt das genauso, wenn man die Länge auf das nächste Vielfache auffüllt („Padding“); die Spaltentransposition mit nicht aufgefülltem Text, also unterschiedlich langen Spalten, ist aber auch nur unwesentlich komplizierter.

Dass die Spaltentransposition den Text über die Gesamtlänge permutiert, sieht auf den ersten Blick sicherer aus, ist aber jetzt als eine *illusorische Komplikation* entlarvt.