$$\underline{RS} = \begin{pmatrix} 01 & a4 & 55 & 87 & 5a & 58 & db & 9e \\ a4 & 56 & 82 & f3 & 1e & c6 & 68 & e5 \\ 02 & a1 & fc & c1 & 47 & ae & 3d & 19 \\ a4 & 55 & 87 & 5a & 58 & db & 9e & 03 \end{pmatrix}$$

$$\begin{pmatrix} s_{i,0} \\ s_{i,1} \\ s_{i,2} \\ s_{i,3} \end{pmatrix} = \underline{RS} \cdot \begin{pmatrix} m_{8i+0} \\ m_{8i+1} \\ \cdots \\ m_{8i+6} \\ m_{8i+7} \end{pmatrix} \tag{10.2}$$

$$\begin{aligned} S_i &= \sum_{j=0}^{3} s_{i,j} \cdot 2^{8j} \qquad i = 0, 1, ..., k-1 \\ S &= (S_{k-1}, S_{k-2}, ..., S_1, S_0) \end{aligned}$$