DES-Verfahren

Rechnen Sie für $f:(x_1,x_2,x_3,x_4)^T \mapsto (x_4,x_3,x_2,x_1)^T$, den geheimen Schlüssel $\vec{k}:=(0,1,0,1)^T$ und die Nachricht $\vec{m}:=(1,1,1,0)^T$ die prototypische DES-Ver- und Entschlüsselung nach.

$DES: \mathbb{Z}_2^4 \to \mathbb{Z}_2^4,$

$(m_1,\dots,m_4)^T \mapsto (f^{-1} \circ u_2 \circ t \circ u_1 \circ f)(m_1,\dots,m_4)$

$DES^{-1}: \mathbb{Z}_2^4 \to \mathbb{Z}_2^4,$

$(c_1,\dots,c_4)^T \mapsto (f^{-1} \circ u_1 \circ t \circ u_2 \circ f)(c_1,\dots,c_4)$

$t: \mathbb{Z}_2^4 \to \mathbb{Z}_2^4,\ (x_1,\dots,x_4)^T \mapsto (x_3, x_4, x_1, x_2)^T$

$s_1: \mathbb{Z}_2^2 \to \mathbb{Z}_2^2,\ (x_1,\dots,x_2)^T \mapsto (x_1,\dots,x_2)^T + (k_1,\dots,k_2)^T$

$s_2: \mathbb{Z}_2^2 \to \mathbb{Z}_2^2,\ (x_3,\dots,x_4)^T \mapsto (x_1,\dots,x_2)^T + (k_3,\dots,k_4)^T$

$u_1: \mathbb{Z}_2^4 \to \mathbb{Z}_2^4,\ (x_1,\dots,x_4)^T \mapsto (x_1,\dots,x_2,(x_3,\dots,x_4)+s_1(x_1,\dots,x_2))^T$

$u_2: \mathbb{Z}_2^4 \to \mathbb{Z}_2^4,\ (x_1,\dots,x_4)^T \mapsto (x_1,\dots,x_2\ (x_3,\dots,x_4)+s_2(x_1,\dots,x_2))^T$

Verschlüsselung

$\vec{c} = (f^{-1} \circ u_2 \circ t \circ u_1 \circ f)(1,1,1,0)$

$= (f^{-1} \circ u_2 \circ t \circ u_1)(0,1,1,1)$

$= (f^{-1} \circ u_2 \circ t)(\underset{x_1}{0}, \underset{x_2}{1}, \underset{x_3}{1} + \underset{x_1}{0} + \underset{k_1}{0}, \underset{x_4}{1} + \underset{x_2}{1} + \underset{k_2}{1})$ $(0,1,1,1)$

$= (f^{-1} \circ u_2)(\underset{x_3}{1}, \underset{x_4}{1}, \underset{x_1}{0}, \underset{x_2}{1})$

$= f^{-1}(\underset{x_1}{1}, \underset{x_2}{1}, \underset{x_3}{0} + \underset{x_1}{1} + \underset{k_3}{0}, \underset{x_4}{1} + \underset{x_2}{1} + \underset{k_4}{1})$ $(1,1,1,1)$

$= (1,1,1,1)^T \pmod 2$

Entschlüsselung

$\vec{m} = (f^{-1} \circ u_1 \circ t \circ u_2 \circ f)(1,1,1,1)$

$= (f^{-1} \circ u_1 \circ t \circ u_2)(1,1,1,1)$

$= (f^{-1} \circ u_1 \circ t)(\underset{x_1}{1}, \underset{x_2}{1}, \underset{x_3}{1} + \underset{x_1}{1} + \underset{k_3}{0}, \underset{x_4}{1} + \underset{x_2}{1} + \underset{k_4}{1})$ $(1,1,0,1)$

$= (f^{-1} \circ u_1)(0,1,1,1)$

$= (f^{-1})(\underset{x_1}{0}, \underset{x_2}{1}, \underset{x_3}{1} + \underset{x_1}{0} + \underset{k_1}{0}, \underset{x_4}{1} + \underset{x_2}{1} + \underset{k_2}{1})$ $(0,1,1,1)$

$= (1,1,1,0)^T \pmod 2$