Kryptografia
Ćwiczenia 2

2025-10-10

Adrian Herda
Politechnika Wrocławska

1. Zadanie 2

$\Pr[\mathrm{Enc}(k, m_0) = c] = \Pr[\mathrm{Enc}(K, m_1) = c]$, $\cancel{k}$ - uniform distribution

$$\left(\forall_{m_0, m_i \in \mathcal{M}}\right)(\forall_{c \in \mathcal{C}}) \Pr[m = m_0 \mid \mathrm{Enc}(k, m) = c] = \Pr[m = m_0] \tag{1}$$

Proof.

$$\begin{aligned}
\Pr[m = m_0] &= \frac{1}{|m|} \\
\Pr[m = m_0 \mid \mathrm{Enc}(k, m) = c] &= \frac{\Pr[m = m_0 \wedge \mathrm{Enc}(k, m) = c]}{\Pr[\mathrm{Enc}(k, m) = c]} \\
&= \frac{\Pr[m = m_0 \wedge \mathrm{Enc}(k, m_0) = c]}{\sum_{m_i \in M} \Pr[m = m_i \wedge \mathrm{Enc}(k, m_1) = c]} \\
&= \frac{\Pr[m = m_0] \cdot \Pr[\mathrm{Enc}(k, m_0] = c]}{\sum_{m_i \in M} \Pr[m = m_i] \Pr[\mathrm{Enc}(k, m_i) = c]} \\
&= \frac{\Pr[m = m_0] \Pr[\mathrm{Enc}(k, m_0) = c]}{\sum_{m_i \in M} \Pr[m = m_i] \Pr[\mathrm{Enc}(k, m_0) = c]} \\
&= \frac{\Pr[m = m_0]}{\sum_{m_i \in M} \Pr[m = m_i]} = p_0
\end{aligned} \tag{2}$$

■