Úloha č. 1

Mějme $q(n)$ polynomiální horní hranici na délku ciphertextu pro zprávy délky 1. Adversary $\mathbb{A}$ zvolí zprávy m_0 délky 1 a m_1 délky $q(n)+n$. Pokud má obdržený ciphertext c délku větší než $q(n)$, ví $\mathbb{A}$, že $c = E(m_1)$, jinak hádá náhodně. Pravděpodobnost, že $\mathbb{A}$ uhádne zprávu, potom je

$$\begin{aligned}\Pr[b' = b] &= \Pr[b' = b \;\&\; |c| > q(n)] + \Pr[b' = b \;\&\; |c| \leq q(n)] \\ &= \Pr[|c| > q(n)] + 1/2 \cdot (1 - \Pr[|c| > q(n)]) \\ &= 1/2 + 1/2 \cdot \Pr[|c| > q(n)]\end{aligned}$$