Úloha č. 2

Adversary se nejprve pošle šifrovacímu orákulu zprávu $(0^n||0^n)$. Feistelova síť se třemi rundami vrátí ciphertext

$$E_k(0^n||0^n) = (a||b), \begin{cases} a = F_2(F_1(0)), \\ b = F_1(0) \oplus F_3(a). \end{cases}$$

Následně se adversary zeptá dešifrovacího orákula na inverz ciphertextu $(a||0^n)$. Pro Feistelovu síť obdrží

$$D_k(a||0^n) = (c||d), \begin{cases} c = F_3(a) \oplus F_1(d), \\ d = a \oplus F_2(F_3(a)). \end{cases}$$

Všimněme si, že $x := b \oplus c = F_1(d) \oplus F_1(0)$. Nakonec se adversary dotáže šifrovacího orákula na ciphertext zprávy $(x||d)$.

$$E_k(x||d) = (e||f), \begin{cases} e = d \oplus F_2(x \oplus F_1(d)) = d \oplus F_2(F_1(0)) = d \oplus a, \\ f = x \oplus F_1(d) \oplus F_3(e). \end{cases}$$

Vidíme tedy, že pro Feistelovu síť o třech rundách bude vždy platit $e = d \oplus a$. Jelikož pro náhodnou permutaci toto bude platit s pravděpodobností $1/2^n$, máme účinného distinguishera těchto Feistelových sítí, což nám dává spor s tím, že jsou silně pseudonáhodné.