CIn-UFPE
Introdução à Criptografia Moderna (Graduação)
Fundamentos da Criptografia Moderna (Pós-Graduação)
2009.1
Lista de Exercícios 6
Entrega: 5ª feira, 08/05/2009

Exercício 1 (Katz & Lindell (2007), 6.1 (2,0)) Mostre que a função soma $f(x, y) = x + y$ (onde $|x| = |y|$ e x e y são interpretados como números naturais) não é unidirecional. Igualmente, mostre que $f(x) = x^2$ não é unidirecional.

Exercício 2 (Katz & Lindell (2007), 6.4 (2,0)) Prove que se f for uma função unidirecional, então $g(x_1, x_2) = (f(x_1), x_2)$ onde $|x_1| = |x_2|$ também é uma função unidirecional. Observe que g revela completamente metade de seus bits de entrada, mas mesmo assim é unidirecional.

Exercício 3 (Katz & Lindell (2007), 6.5 (2,0)) Seja f uma função unidirecional que preserva o comprimento, e suponha que nd seja um predicado núcleo-duro para f . Defina $G(x) = (f(x), nd(x))$. G é um gerador pseudoaleatório? Prove sua resposta.

Exercício 4 (Katz & Lindell (2007), 6.7 (2,0)) Seja f uma função unidirecional. Será que $g(x) = f(f(x))$ é necessariamente unidirecional? E $g(x) = (f(x), f(f(x)))$? Prove sua resposta.

Exercício 5 (Katz & Lindell (2007), 6.10 (2,0)) Mostre que se uma função injetora tem um predicado núcleo-duro, então ela é unidirecional.