HIT — Cryptography — Homework 3

September 25, 2014

Problem 1. In our attack on a two-round substitution-permutation network, we considered a block length of 64 bits and a network with 16 S-boxes that each take a 4-bit input.

1. Repeat the analysis for the case of 8 S-boxes, each taking an 8-bit input. What is the complexity of the attack now?
2. Repeat the analysis again with a 128-bit block length and 16 S-boxes that each take an 8-bit input.
3. Does the S-boxes length make any difference? Does the block length make any difference?

Problem 2. Show that DES has the property that $DES_k(x) = \overline{DES_{\overline{k}}(\overline{x})}$ for every key k and input x (where $\overline{z}$ denotes the bitwise complement of z). This is called the complementarity property of DES.

Problem 3. Is the addition function $f(x, y) = x + y$ (where $|x| = |y|$ and x and y are interpreted as natural numbers) a one-way function?

Problem 4. Let $f_1(x)$ and $f_2(x)$ be one-way functions. Is $f(x) = (f_1(x), f_2(x))$ necessarily a one-way function? Prove your answers.

Problem 5. Let f be a one-way function. Is $g(x) = f(f(x))$ necessarily a one-way function? What about $g(x) = (f(x), f(f(x)))$? Prove your answers.