HIT — Cryptography — Homework 4

September 4, 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 block length make any difference?

Problem 2. What is the output of an r-round Feistel network when the input is (L_0, R_0) in each of the following two cases: (Show your analysis.) (a) Each round function F outputs all 0s, regardless of the input. (b) Each round function F is the identity function.

Problem 3. 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 4. Prove that if f is a one-way function, then $g(x_1, x_2) = (f(x_1), x_2)$ where $|x_1| = |x_2|$ is also a one-way function. Observe that g fully reveals half of its input bits, but is nevertheless still one-way.

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.

Problem 6. Let G be a pseudorandom generator with expansion factor $\ell(n) = n + 1$. Prove that G is a one-way function.