ECS 227: Modern Cryptography Handout ps2
UC Davis — Phillip Rogaway January 31, 2012

Problem Set 2

Please turn in your solutions at the beginning of class on Thursday, February 9, 2012.

Problem 1. Let $e: \{0,1\}^{56} \times \{0,1\}^{64} \to \{0,1\}^{64}$ be a blockcipher. Define from e a blockcipher $E: \{0,1\}^{112} \times \{0,1\}^{64} \to \{0,1\}^{64}$ by asserting that $E_{k_1 k_2}(x) = e_{k_2}(e_{k_1}(x))$. You are given a few plaintext/ciphertext pairs (x_i, y_i) for $y_i = E_{k_1 k_2}(x_i)$. Describe and analyze the best attack you can find that, with high probability, will find k_1, k_2. Your attack should use far fewer than 2^{112} computations of e (closer to 2^{56}). Make, and state, any reasonable assumption you find necessary to solve this problem.

Problem 2. Let E be a blockcipher on 20 bits that is defined by using eight rounds of balanced Feistel, each round based on a random round function $F_i\colon \{0,1\}^{10} \to \{0,1\}^{10}$. Describe an information-theoretic attack[1] that, asking a small number of queries, distinguishes E from a random permutation on 20 bits. How many queries did you need to ask to carry out your attack?

Now attending to the time complexity of your attack, estimate how many steps a direct implementation of your attack would take to run.

Problem 3. Suppose you are given a PRP $e\colon \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. Based on it, describe two or three completely different constructions for a PRP $E\colon \mathcal{K} \times \{0,1\}^{2n} \to \{0,1\}^{2n}$. Your constructions should plausibly be PRP-secure if e is PRP-secure, but you need not prove this to be true.

Problem 4. Consider the following two ways to instantiate a pair of oracles $f, g\colon \{0,1\}^n \to \{0,1\}^n$.

(1) f is a random function on n bits, k is a random n-bit string, and $g(x) = f(x \oplus k)$.

(2) f and g are random, independent functions from n bits to n bits.

Suppose an adversary A makes at most q queries. Use a game-playing argument to upperbound

$$\Pr_1[A^{f,g} \Rightarrow 1] - \Pr_2[A^{f,g} \Rightarrow 1]$$

where the first probability is with respect to the first method of instantiating f and g and the second probability is with respect to the second way of instantiating f and g.

[1] That is, do not concern yourself with the time complexity of the attack.