CS195-7: Introduction to Cryptography DUE: November 12, 2002

Problem Set 7

Instructor: Anna Lysyanskaya

PRF Candidates

Suppose that $\{F_S : \{0,1\}^k \mapsto \{0,1\}^k \mid s \in \{0,1\}^k\}$ is a pseudo-random family of functions from k-bit input to k-bit output, indexed by a k-bit key ("seed"). We would like to construct a new PRF family. Consider the following constructions, and for each show whether it is good or bad (namely whether the specified family is pseudo-random or not, for the appropriate domain and range). If your answer is "yes," give an outline of a reduction. If your answer is "no," give an example F, some convincing evidence that F is a PRF, and an attack on the construction of F^i when it is based on your F.

Below, "$\circ$" denotes concatenation, and $\bar{x}$ denotes the bitwise negation of x.

(a) $F_S^1(x) = F_S(x) \circ F_S(\bar{x})$.

(b) $F_S^2(x) = F_{0^k}(x) \circ F_S(x)$.

(c) $F_S^3(x) = F_{S_1}(x) \circ F_{S_2}(x)$, where $S_1 = F_S(0^k)$ and $S_2 = F_S(1^k)$.

(d) $F_S^4(x) = F_S(x) \oplus x$.

(e) $F_S^5(x) = F_S(x) \oplus S$.