University of Maryland
CMSC456 — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 3

Due at *beginning* of class on Oct. 18

1. Let $P : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^m$ be a (t,ϵ)-PRP. Consider the encryption scheme defined as follows: the sender and receiver share in advance a randomly-chosen key $s \in \{0,1\}^k$. To encrypt a message $M \in \{0,1\}^{m/2}$, the sender chooses a random "padding" $r \in \{0,1\}^{m/2}$, concatenates r and M, and sends $C = P_s(r \circ M)$.

   (a) How can decryption be performed in the above scheme?

   (b) Consider the security of the above scheme in the sense of left-or-right indistinguishability. Specifically, bound the success probability of any adversary A (running in time at most t) attacking the above scheme.

   (c) We can modify the above scheme to support encryption of m-bit messages in the following way: to encrypt an m-bit message M, simply break M in two parts M_1, M_2 and separately encrypt both halves. In class we gave the following encryption scheme for m-bit messages: $\langle r, P_s(r) \oplus M \rangle \leftarrow \mathcal{E}_s(M)$. Discuss the relative merits of these two encryption schemes for m-bit messages in terms of ciphertext length, security, and necessary conditions on P.

2. Let $F : \{0,1\}^k \times \{0,1\}^m \to \{0,1\}^n$ be a (t,ϵ)-PRF. Define keyed function $P : \{0,1\}^k \times \{0,1\}^{m+n} \to \{0,1\}^{m+n}$ as follows (where $|x| = m$ and $|y| = n$):

$$P(s, x \circ y) = (F(s,x) \oplus y) \circ x,$$

   (a) Show that P is a keyed *permutation*.

   (b) Show how to efficiently compute P_s^{-1} (for any s) even though F_s^{-1} might not be efficiently computable.

   (c) Show that P is *not* a PRP by giving an explicit algorithm A that distinguishes it from a random permutation (hint: you can do this with an A that makes only a single query to its oracle).

   (d) Graduate students only. Iterate the above process one more time, giving:

$$P'(s_1 \circ s_2, x \circ y) = P(s_2, (F(s_1,x) \oplus y) \circ x) = (F(s_2, (F(s_1,x) \oplus y)) \oplus x) \circ (F(s_1,x) \oplus y).$$

   As before, show that $P' : \{0,1\}^{2k} \times \{0,1\}^{m+n} \to \{0,1\}^{m+n}$ is a keyed permutation, that P'^{-1}_s can be efficiently computed, and that P' is *not* a PRP (here, your algorithm A will need to ask more than one query).

   Note: iterating a third time *does* yield a provably-secure PRP!