Due dates. If submitting by email (teshrim@ufl.edu), the assignment is due by 6pm on Wednesday 1/25. You may submit a hardcopy in class if you prefer, but please only submit one way or the other.

Problem 1. Fix $k, n > 0$ and let $E: \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$ be a blockcipher. Let’s say you are concerned about its hardness against key-recovery attacks. In particular, you are worried that an exhaustive key-recovery attack will take significantly less that $2^k$ work. So you define $F: \{0,1\}^{k+n} \times \{0,1\}^n \rightarrow \{0,1\}^n$ by $F(K_1 \parallel K_2, X) = E_{K_1}(X \oplus K_2)$, where $K_1 \in \{0,1\}^k$ and $K_2 \in \{0,1\}^n$. Notice that $F$ is a blockcipher with a $(k+n)$-bit key and an $n$-bit blocksize.

For purpose of analysis, let’s model $E$ as an “ideal cipher”, meaning that $E \leftarrow$ BC$(k,n)$. Given that, what is the complexity of an exhaustive key-search attack on $F$? Naively, you would iterate through every possible $(k+n)$-bit key to $F$, which would require making $2^{k+n}$ evaluations of $F$. (Or $F^{-1}$ if you prefer that direction. Note that if you are doing exhaustive key search, you’re just running the blockcipher locally as you work through the key space. So you can run it forwards or backwards, as you like.) The question is: can you recover the key $K_1 \parallel K_2$ (with overwhelming probability) using significantly fewer than $2^{k+n}$ calls to $F/F^{-1}$? If you can, then going from a $k$-bit key to a $(k+n)$-bit key hasn’t really gained much...

If you don’t recall the specifics of the exhaustive key-search attack, watch that portion of the Lecture 2 video again.

Problem 2. BR notes\(^1\), Chapter 3: problem 1. Carefully describe your adversary, and give the PRP advantage of it. Please use the notation we use in class when describing the adversary, when writing experiments, advantage, etc.

Problem 3. BR notes, Chapter 3: problem 6. Here you must give a security reduction! Since this is your first one, I’ll get you started. Given an adversary $A$ that attacks the PRP-security of $E^{(2)}$, build an adversary $B$ that attacks the PRP-security of $E$. Carefully show that the PRP-advantage of $B$ upperbounds the PRP-advantage of $A$, by analyzing the probability that $B$ “wins” its experiment. When building your adversary $B$, try to make it as simple as possible, and as parsimonious as possible with respect to its resources. Finally, write a nice theorem statement to encapsulate your result.

\(^1\)https://cseweb.ucsd.edu/~mihir/cse207/w-prf.pdf