Problem Set 2

Please turn in your solutions at the beginning of class on Wednesday, February 5, 2014. Remember that you can work with others, if you wish.

Problem 1. Suppose $G\colon \{0,1\}^n \to \{0,1\}^N$ is a good PRG, according to the prg-notion defined in class. Which of the following are necessarily good PRGs as well, according to the prg-notion defined in class? (You can infer the intended signature of G' in each case.) Briefly explain each answer.

- $G'(s) = G(s)[1..N-2]$ (ie, discard the last two bits. Assume $N \geq n+3$)
- $G'(s \parallel s') = G(s) \parallel G(s')$ (where $|s| = |s'|$)
- $G'(s) = G(s) \oplus 1^N$
- $G'(s) = G(s) \oplus G(s+1)$ (with implicit type conversion for this to make sense)
- $G'(s) = (G(s))^R$ (the reversal of the string)
- $G'(s) = G(s) \parallel 000$

Problem 2. Suppose $F\colon \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^N$ is a good PRF, according to the prf-notion defined in class. Which of the following are necessarily good PRFs as well, according to the prf-notion defined in class? (You can infer the intended signature of F' in each case.) Briefly explain each answer.

- $F'_k(x) = \overline{F_k(x)}$ (bitwise complement)
- $F'_k(x) = F_{\overline{k}}(x)$
- $F'_k(x)$ is $F_k(x)$ if $k \neq 0^\kappa$ and 0^N otherwise
- $F'_k(x)$ is $F_k(x)$ if $x \neq 0^n$ and 0^N otherwise
- $F'_{k1\,k2}(x) = F_{k1}(x) \parallel F_{k2}(x)$ (where $|k1| = |k2|$)
- $F'_k(x) = F_k(x \parallel 0) \parallel F_k(x \parallel 1) \parallel \cdots \parallel F_k(x \parallel 255)$ (where each number i is encoded as a byte)

Problem 3. 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 4. 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.

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