CS 120/CSCI E-177: Introduction to Cryptography

Problem Set 3

Assigned: Oct. 12, 2006 | Due: Oct. 18, 2006 (1:10 PM)

Justify all of your answers. See the syllabus for collaboration and lateness policies. You can submit by email to `ciocan@eecs` (please include source files) or by hardcopy Carol Harlow in MD 343.

Problem 1. (Breaking Some Stream Ciphers)

1. Define $G(x) = y_0 \dots y_n$, where $x = x_0 \cdots x_{n-1}$, $y_0 = x_0$, $y_i = x_{i-1} \oplus x_{i \bmod n}$ for $i = 1, \dots, n$. Show that G is *not* a pseudorandom generator. Also show that the encryption scheme based on G, where $E_k(m) = m \oplus G(k)$, is not computationally secure (i.e. does not have computationally indistinguishable encryptions).

In the remainder of the problem, you will generalize the above to *any* pseudorandom generator for which each bit of output depends on at most two bits of the seed. That is, for every n and every $i \in \{1, \dots, \ell(n)\}$ (where ℓ is the expansion function of G), there exist $j, k \in \{1, \dots, n\}$ and a function f such that $G(x)_i = f(x_j, x_k)$ for all $x \in \{0,1\}^n$. (In contrast, a remarkable result from 2004 shows how to convert essentially any pseudorandom generator into one where every output bit depends on only *four* bits of the seed.)

2. Show that if G is a pseudorandom generator such that each bit of the output depends on at most two bits of the seed, then in fact each bit of the output is equal to either some bit of the seed, the complement of some bit of the seed, the xor of two bits of the seed, or the complement of the xor of two bits of the seed. That is, the functions $f(x_j, x_k)$ must be one of x_j, $\neg x_j$, x_k, $\neg x_k$, $x_j \oplus x_k$, or $\neg(x_j \oplus x_k)$. (Hint: what property do all 2-bit functions other than these have?)

3. Show that there does not exist a pseudorandom generator such that each bit of the output depends on at most two bits of the seed. Also show that the encryption scheme based on G, where $E_k(m) = m \oplus G(k)$, is not computationally secure. (Hint: After using Part 2, we can define a set $S = \{j : x_j \text{ or its complement is an output bit of } G\}$ and a graph H with edge set $\{(j,k) : x_j \oplus x_k \text{ or its complement is an output bit of } G\}$. Use the expansion of G to argue that either H contains a cycle or there are two elements of S connected by a path in H.)

Problem 2. (Guessing Indistinguishability $\Rightarrow$ Indistinguishability) In class, we showed that if an encryption scheme has computationally indistinguishable encryptions then it also satisfies guessing indistinguishability. Show that the converse of this statement is also true.

Problem 3. (Properties of Pseudorandom Sequences) Let G be a pseudorandom generator with expansion function ℓ. Show that $G(U_n)$ has a sequence of at least $2 \log_2 \ell(n)$ consecutive ones with low probability (i.e. tending to 0 as $n \to \infty$). Can this probability be negligible?

Problem 4. (Key recovery in secure encryption) Let (G, E, D) be a computationally secure encryption scheme over the message space $\{0,1\}^n$. Show that the probability that a PPT adversary can recover the key after seeing the encryption of a random message (uniformly distributed in $\{0,1\}^n$) is negligible. (Hint: use semantic security.)