CSE 599b | Cryptography | Winter 2006

Problem Set 1 Due: Friday, Feb 10

January 25, 2006

Solve as many of the problems below as you can. You should attempt at least three of them.

1. In using an n-bit block cipher for symmetric encryption, an alternative to cipher-block chaining with a random IV might be to use an n-bit counter c of the number of blocks that have previously been sent (over the entire course of Alice and Bob's communication) as follows: This counter c is maintained by both parties and starts off at 0^n. To encrypt the block indexed by c, M_c, Alice sends $C = E_K(M_c \oplus c)$ and then increments her copy of c. To decrypt, Bob computes $E_K^{-1}(C) \oplus c$ and then increments his copy of c. Show that such a scheme is insecure under a reasonable definition of security.

2. (Equivalence of one-way functions and collections of one-way functions)
   (a) Show, given a one-way function, how to construct a collection of one-way functions.
   (b) *Show, given a collection of one-way functions, how to construct a one-way function. (Hint: You may need the randomness in your sampling algorithms as part of your input.)

3. (Random Self-reduction) Suppose that you have a family of functions $\{f_i : D_i \to R_i\}_{\{i \in I\}}$ that satisfies the conditions below (i.e. is a collection of weak one-way homomorphisms on groups whose operations are polynomial-time computable and that have uniform sampling) then it is also a collection of (strong) one-way functions.
   - There is a sampling algorithm C_I that on input 1^n samples $i \in I \cap \{0,1\}^n$.
   - There is a sampling algorithm S_D that on input i samples x *uniformly* from D_i.
   - There is a polynomial-time algorithm F that on input $i \in I$ and $x \in D_i$ computes $f_i(x)$.
   - $(D_i, \bullet_i)$ and $(R_i, \circ_i)$ are groups whose group operations $\bullet_i$ and $\circ_i$ and group inverses are polynomial-time computable.
   - f_i is a homomorphism from $(D_i, \bullet_i)$ to $(R_i, \circ_i)$.
   - There is some c such that for all PPT A,

   $$\epsilon(n) = \Pr[A(f_i(x), i) \in f_i^{-1}(f_i(x)) \mid i \leftarrow C_I(1^n); x \leftarrow S_D(i)]$$

   satisfies $\epsilon(n) \leq 1 - 1/n^c$.

   (Hint: Show how to take an algorithm that inverts f_i on a $1/n^c$ fraction of inputs in D_i and use the group properties to invert f_i almost surely on random elements of D_i.)

4. In this problem you will derive a weak version of the Prime Number Theorem that is sufficient for all cryptographic applications.

   (a) Show that for any prime p, the largest power of p that divides $n!$ is

   $$\lfloor\frac{n}{p}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \cdots + \lfloor\frac{n}{p^r}\rfloor$$

   where r satisfies, $p^r \leq n < p^{r+1}$.

   (b) Show that for any $m \geq 1$, $\lfloor\frac{2n}{m}\rfloor \leq 2\lfloor\frac{n}{m}\rfloor + 1$.

   (c) Use the results of parts (a) and (b) to show that for any prime p, the largest power p^r of p that divides $\binom{2n}{n}$ satisfies $p^r \leq 2n$.

   (d) Prove that for any integer $n \geq 1$, $\binom{2n}{n} \geq 2^n$. (It actually is $\Theta(2^{2n}/\sqrt{n})$.)

   (e) Use the lower bound on the size of $\binom{2n}{n}$ from part (d) and upper bound on each of its prime power factors from part (c) to prove that the number of distinct primes dividing $\binom{2n}{n}$ is at least $n/\log_2(2n)$.

   (f) Conclude that there are at least $n/\log_2(2n)$ primes less than $2n$.

5. Prove that if f is a one-way function that is a permutation on every $\{0,1\}^n$ and B is a polynomial-time computable hard-core bit for f then the function $G : \{0,1\}^* \rightarrow \{0,1\}^*$ given by $G(x) = f(x)B(x)$ is a pseudorandom generator.