CS 120/CSCI E-177: Introduction to Cryptography

Problem Set 4

Assigned: Oct. 26 Due: Nov. 1, 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. (Factoring vs. block ciphers)

1. The General Number Field Sieve algorithm is (asymptotically) the fastest algorithm known for integer factorization. Heuristically, factoring an integer N with it takes time proportional to:
$$L(N) = \exp\left(c \cdot (\ln N)^{\frac{1}{3}} \cdot (\ln \ln N)^{\frac{2}{3}}\right),$$
where $c \approx 1.526$. In 2005, a 640-bit integer was factored in 3 months using 80 2.2GHz PCs. Using the same hardware, what is the time for factoring a 1024-bit integer (as well as you can estimate given the information in this problem)? And a 2048-bit integer?

2. The best known attack against some block ciphers is essentially a brute-force search of the key space. In 1999, a specialized key-search machine costing $250,000 cracked a 56-bit DES key in 56 hours. Using similar hardware, what is the time to break a 96-bit key? a 128-bit key?

3. What other criteria would you take into account when deciding how long to make your composite numbers or block-cipher keys for cryptography?

Problem 2. (Computational Number Theory) Do everything in this problem *by hand* and show your work.

1. Read about the extended GCD algorithm in Katz–Lindell (§8.1). Apply it to the primes 53 and 71.

2. What is the inverse of 53 modulo 71?

3. Calculate the Chinese Remainder coefficients for $53 \cdot 71 = 3763$, and find the element of $\mathbb{Z}_{3763}$ corresponding to $(10, 6) \in \mathbb{Z}_{53} \times \mathbb{Z}_{71}$.

4. Find all square roots of 25 in $\mathbb{Z}_{3763}$. (Hint: first find all the square roots of 25 in $\mathbb{Z}_{53}$ and $\mathbb{Z}_{71}$.)

5. Find all generators g of $\mathbb{Z}_7^*$, and find $\log_g 3$ for each of them.

Problem 3. (More candidate one-way functions) Which of the following functions are likely to be one-way functions (or collections of one-way functions, in the case of Parts 3 and 4)? Justify your answers by either giving a polynomial-time adversary that inverts the function with nonnegligible probability or by showing that the function's one-wayness follows from the one-wayness of one of the candidates given in class.

1. $f(x) = x^2$, where x is an integer.
2. $f(x, y) = x \cdot y - 2^{\lceil \|x\|/2 \rceil} \cdot y$, where $\|x\| = \|y\|$.
3. $f_N : \mathbb{Z}_N \to \mathbb{Z}_N$ defined by $f_N(x) = x^2 + 2x \bmod N$, where $N = pq$ for random n-bit primes p, q.
4. $f_{p,x} : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ defined by $f_{p,x}(y) = y^x \bmod p$, where p is a random n-bit prime and $x \xleftarrow{R} \{0, \ldots, p-2\}$.
5. $f(x_1, \ldots, x_n, S) = (x_1, \ldots, x_n, \sum_{i \in S} x_i \bmod n^2)$, where each $x_i \in \{1, \ldots, n^2\}$ and $S \subseteq \{1, \ldots, n\}$.
6. Extra credit: $f(x_1, \ldots, x_n, S) = (x_1, \ldots, x_n, \sum_{i \in S} x_i)$, where each $x_i \in \{1, \ldots, n^2\}$ and $S \subseteq \{1, \ldots, n\}$.