T-79.159 Cryptography and Data Security **Spring 2003**
Tutorial 5
Tue 11.3.2003 12–14 T3 or Wed 12.3.2003 18–20 T1

1. Let $f\colon \{0,1\}^n \to \{0,1\}^n$ be a one-way function. Is $f^*\colon \{0,1\}^n \to \{0,1\}^n$ defined by $f^*(x) = f(x) \oplus x$ always a one-way function?

2. Let $h\colon \{0,1\}^n \to \{0,1\}^m$ with $m < n$ be a hash function. Suppose that h is collision resistant. Is it also one-way?

   Hint: suppose you have an algorithm that inverts h. Use this algorithm to construct an algorithm for finding collisions.

3. Compute $5^{12345678} \bmod 100000007$.

4. Compute the following inverses using the Euclidean algorithm:

   (a) $5^{-1} \pmod{274}$, and

   (b) $278^{-1} \pmod{1155}$.

5. Let $n = pq$, where $p \neq q$ are primes. Recall that the Euler ϕ function of n is defined by $\phi(n) = (p-1)(q-1)$. Suppose that you know n and $\phi(n)$. How can you efficiently factor n based on this information?

   Thus, factoring n and computing $\phi(n)$ are equivalent problems.