INTRODUCTION TO MODERN CRYPTOGRAPHY
HOMEWORK I

Three simple rules. You can discuss homework with other students. You can consult any book, article, or oracle. You must write the solutions by yourself. If you don't have a solution, you can write your attempts and discuss why they failed.

1. Perfect Secrecy

(1) When using one-time pad with key $k = 0^\ell$, it follows that $\mathsf{Enc}(k, m) = m$ and the message is effectively sent in clear. It has therefore been proposed to improve the one-time pad by having Gen to pick $k \neq 0^\ell$ at random. Is the new encryption scheme still perfectly secure? This is Exercise 2-3 from KL.

(2) Prove or refute: Every encryption schme for which the size of the key space equals the size of the message space and for which the key is chosen uniformly from the key space is perfectly secure. This is Exercise 2-5 from KL.

2. One-way functions and pseudorandom generator

(3) Let f be a one-way function. Is $g(x) = f(f(x))$ necessarily a one-way function? What about $g(x) = (f(x), f(f(x))$? This is Exercise 6-7 from KL.

(4) Let $G : \{0,1\}^n \to \{0,1\}^{n+1}$ be a pseudorandom generator. Prove that G is a one-way function. This is Exercise 6-20 from KL.

Date: April 19, 2008. Due May 1, 2008.