

(Corrected) Exercise Set 5.**Due in Class on Friday, May 4, 2001**

These two problems require a little number-crunching but all of you are used to that!

Write as if this were part of your resume for a high-paying job you really want!

1. (Zero Knowledge proofs) Let $n = 437 = 19 \times 23$. Convince me that you know the factors 19 and 23 of 437, without disclosing them to me, if I send you the following fourth power modulo 437: 150.

2. (Secret Sharing) Consider the primes $m_1 = 101$, $m_2 = 103$, $m_3 = 107$, $m_4 = 109$, $m_5 = 113$. The integer x (*appropriately chosen for these parameters*) represents the combination to open a bank vault. The integer x is congruent to 11, 66, 22, 24, and 76 modulo 101, 103, 107, 109, and 113, respectively, and these five pieces of information are given to five different people of the Executive Board of the bank. If the three people holding the information 66, 24, and 76 decide to collaborate, what is the combination to the vault? If only the people holding the information 66 and 24 cooperate, what are the possibilities for the combination?