

Solutions to 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!

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.

So we know the 4th power of some number x modulo 437: $x^4 = 150 \% 437$. Since we also know that $437 = 19 \times 23$, we can find the principal square roots modulo 19 and 23 (necessarily x^2 , since the principal square root modulo primes equal to 3 modulo 4 is the square root that itself has a square root - which x^2 obviously does). Calculating these principal square roots we get

$$y_1 = (150)^{(19+1)/4} = 150^4 = 6 \% 19 \text{ and } y_2 = (150)^{(23+1)/4} = 150^6 = 9 \% 23.$$

Finding the multiplicative inverse of 19 mod 23 and 23 mod 19, using the Euclidean algorithm we get

$$1 = 5 \times 23 - 6 \times 19.$$

Then we determine that

$$y = x^2 = 6(5 \times 23) + 9(-6 \times 19) = 101 \% 437.$$

You send 101 to me which, after computing $x^2 \% 437$, knowing x , leads me to conclude that you knew the factorization of 437.

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?

We have $M' = (103)(109)(113) = 1,268,651$ and

$$M'_1 = (109)(113) = 12,317, \quad M'_2 = (103)(113) = 11,639, \quad M'_3 = (103)(109) = 11,227.$$

The multiplicative inverses n_i of M'_i modulo m_i are calculated to be (Euclidean algorithm)

$$n_1 = 91\%103, \quad n_2 = 59\%109, \quad n_3 = 65\%113.$$

We now know that the secret number x satisfies

$$x = \sum_{i=1}^3 a_i(M_i n_i) = 23,241 \bmod 1,268,651.$$

Since x is chosen to be less than the product of the smallest three m_i 's, we know that $x = 23,241$.

The second part of the problem is done in a similar way using only two a_i 's in which case we get that $x = 787 \bmod 11,227$. But we cannot narrow x down to a single number, but only know it is of the form $11,227 \times m + 787$ and in the chosen interval.