Security

Assignment 12, Thursday 18 December, 2008

Goals: After successfully completing this exercise you should have a working grasp of the elementary number theory that are used in cryptography.

Deadline: Friday January 9 or earlier. You have to send your answers to **Olha**, by e-mail or to the post-box. **Attention: Flavio is in ARGENTINA. He tells that he is not reachable by e-mail or any other way.**

1. (2 points) *Prime divisors* and *greatest common divisor* ($\mathsf{gcd}(x, y)$).
   - The prime-divisor factorisation of 24 is $2^3 \times 3$. Find the factorisation of 30, then find $\mathsf{gcd}(24, 30)$, and then factorise $\mathsf{gcd}(24, 30)$.
   - Factorise 15 and 8. Find $\mathsf{gcd}(15, 8)$, and then factorise it in terms of the prime divisors 2, 3 and 5. You may use zero-degrees: 2^0, 3^0, 5^0.
   - Let $x = {p_1}^{n_1} \times \ldots \times {p_k}^{n_k}$ and $y = {p_1}^{m_1} \times \ldots \times {p_k}^{m_k}$ be factorisations of x and y respectively, where some of n_i or m_j may be 0. What is the factorisation of $\mathsf{gcd}(x, y)$?
2. (1 point) *Euler totient function* ϕ.
   - Name the elements of the set $\{1, \ldots, 5\}$ that are relatively prime to 5. What is $\phi(5)$?
   - Name the elements of the set $\{1, \ldots, 9\}$ that are relatively prime to 9. What is $\phi(9)$?
3. (2 points) Let $a \in Z_n$. The *multiplicative inverse* x of the number a is such that $ax \equiv 1 (\mathsf{mod}\ n)$ holds.
   - Why can you look for x using the formula $x = \dfrac{nk+1}{a}$, for some $k = 0, 1, 2, \ldots$?
   - Find x such that $7x \equiv 1 (\mathsf{mod}\ 8)$ holds.
   - Let $a = n - 1$. Find x such that $(n-1)x \equiv 1 (\mathsf{mod}\ n)$. Explain your answer.
4. (3 points) *Multiplicative groups.*
   - Look at the multiplication table for ${Z^*}_{15}$ (Lecture 13 of Aspinall). Find the order of each element.
   - Create the multiplication table for ${Z^*}_6$. What are the orders of its elements? Is this group cyclic or not (and why)? If"yes", what are the generators?
5. (2 points) *Chinese Remainder Theorem.*
   - Show that for co-prime n and m the map $\varphi : Z_{nm} \to Z_n \times Z_m$, where

     $$\varphi(x) = (x \mod n, x \mod m)$$

     is a bijection. Hint: you have to show that φ is everywhere defined (trivially by the definition), functional (that is for any x there is only one image; trivially by the def.), injective and surjective.
   - Let $n = 15$ and $m = 4$. Find the φ-preimage of $(7, 2)$ in Z_{60}, that is such $x \in Z_{60}$ that $\varphi(x) = (7, 2)$.