Wrocław University of Technology, WPPT 23.10.13

CRYPTOGRAPHY, 2013 Assignments, list # 4

1. Find and prove the recursive formula for finding x, y such that

   $$x \cdot a + y \cdot b = GCD(a, b)$$

   using extended Euclidean algorithm.

   Use this method to find modular inverse modulo n: that is for $a < n$ such that a and n are coprime (i.e. they have no common divisors), find b such that $a \cdot b = 1 \bmod n$.

2. Let $\mathbb{Z}_n^*$ denote the elements in the set $\{1, \ldots, n-1\}$ which are coprime with n. Show that $\mathbb{Z}_n^*$ is a group with multiplication modulo n.

   For RSA number $n = pq$ show that the number of elements of $\mathbb{Z}_n^*$ is $(p-1)(q-1)$. Show that for each $a \in \mathbb{Z}_n^*$ we have $a^{(p-1)(q-1)} = 1 \bmod n$.

3. Let n, d, e be RSA keys. Show that $m^{de} = m \bmod n$ even if $m < n$ is not coprime with n.

4. Show that finding a private key e corresponding to the RSA public key n, d is equivalent to factorization of n.

   Is finding the plaintext m for a ciphertext $m^d \bmod n$ from n and d equivalent to factorization?

5. Let n be an RSA number. For how many elements $x < n$ we have $x^2 = 1 \bmod n$.

   Let $a < n$. Determine the number of square roots of a modulo n, that is the number of elements y such that $y^2 = a$

6. Let n be an RSA number. Show that one can find factorization of n, if one can find square roots modulo n.

7. How many elements are contained in $\mathbb{Z}_{n^2}^*$?

   Show that $(n+1)^x = 1 + nx \bmod n^2$ for any x.

/-/ Mirosław Kutyłowski and Maciej Gebala