Homework 1 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

19.04.2007

Exercise 1. The ElGamal cryptosystem requires the computation of primitive elements modulo a prime p. If we are able to factor $p-1$, the following statement offers a method to determine whether a given number a is a primitive element modulo p. Prove this statement:

Let p be an odd prime and let the prime factorization of $p-1$ be

$$p-1=\prod_{i=1}^{r} p_i^{e_i}.$$

A number $a \in \mathbb{Z}_p^*$ is a primitive element modulo p if and only if for all $i \in \{1,\ldots,r\}$

$$a^{p-1/p_i} \not\equiv 1 \bmod p.$$

Exercise 2. Let p be prime, g a primitive element modulo p and $a,b \in \mathbb{Z}_p^*$.
Show the following:

(a) a is a quadratic residue modulo p, if and only if there exists an even $i \in \mathbb{N}_0$ with $a = g^i \pmod p$.

(b) If p is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo p.

(c) The product ab is a quadratic residue modulo p if and only if a and b are both either quadratic residues or quadratic non-residues modulo p.

Exercise 3. Assume that the same message m is encrypted using the RSA cryptosystem, once using the public key (n,e) and once using the public key (n,f). Let $\gcd(e,f)=1$. How can the message be computed from the knowledge of both ciphertexts and the public keys?