Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 11

Friday, July 8, 2016

Problem 1. (*number of Primitive Elements Modulo n*) Prove the following statement:

If there exists a primitive elements modulo n, then there are $\varphi(\varphi(n))$ many.

Problem 2. *(Shamir no-key protocol)* Alice and Bob are using Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31337$ for their communication. Alice chooses the random number $a = 9999$ while Bob chooses $b = 1011$. Alice's message is $m = 3567$.

a) Calculate all exchanged values c_1, c_2, and c_3 following the protocol.
Hint: You may use $6399^{1011} \equiv 29872 \pmod{31337}$.

Problem 3. *(RSA encryption)* A uniformly distributed message $m \in \{1, \dots, n-1\}$ with $n = p\,q$ with two primes $p \neq q$ is encrypted using the RSA-algorithm with public key (n, e).

a) Show that it is possible to compute the secret key d if m and n are not coprime, i.e., if $p \mid m$ or $q \mid m$.

b) Calculate the probability for m and n having common divisors.

c) How large is the probability of (b) roughly, if n has 1024 bits and the primes p and q are approximately of same size ($p, q \approx \sqrt{n}$).

Problem 4. *(Euler-Phi and RSA)*

Let u and v be distinct odd primes, and let $n = u \cdot v$. Furthermore, suppose that an integer x satisfies $\gcd(x, u \cdot v) = 1$.

a) Show that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{u}$ and $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{v}$.

b) Show that $x^{\frac{1}{2}\varphi(n)} \equiv 1 \pmod{n}$.

c) Show that if $ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)}$ holds for two integers d and e, then we obtain $x^{ed} \equiv x \pmod{n}$.