Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 1

Friday, October 20, 2017

Problem 1. *(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 2. *(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 $x^{ed} \equiv x \pmod{n}$.

Problem 3. *(Rabin cryptosystem)* Alice and Bob are using the Rabin Cryptosystem. Bob uses the public key $n = 4757 = 67 \cdot 71$. All integers in the set $\{1, \dots, n-1\}$ are represented as a bit sequence of 13 bits. In order to be able to identify the correct message, Alice and Bob agreed to only send messages with the last 2 bits set to 1. Alice sends the cryptogram $c = 1935$. Decipher this cryptogram.

Problem 4. *(coin flipping)* Consider the coin flipping protocol. Let $p > 2$ be prime.

a) Show that if $x \equiv -x \mod p$, then $x \equiv 0 \mod p$.

b) Suppose Alice cheats when flipping coins over the telephone by choosing $p = q$. Show that Bob almost always loses if he trusts Alice.

c) Alice chooses $n = p^2$ as the secret key, but Bob suspects that Alice has cheated. Can Bob discover her attempt to cheat? Can Bob use Alice' cheating as an advantage for himself?