New RSA Vulnerabilities Using Lattice Reduction Methods

Alexander May

Abstract

In this dissertation thesis we study todays most popular and widely used public-key cryptosystem: the RSA-cryptosystem, which was proposed in 1978 by Rivest, Shamir and Adleman. We show that some choices of the RSA-parameters lead to polynomial time attacks on the cryptosystem.

Let us have a closer look at the parameter generation process in RSA: One chooses two large prime numbers p and q and computes their product $N = pq$. The so-called RSA modul N is public, whereas the factorization of N is kept secret. Furthermore, one chooses a key-pair (e, d) satisfying $ed = 1 \bmod (p-1)(q-1)$. The parameter e is public and the parameter d is secret.

One can easily compute the secret key d from the public information (N, e) if the factorization of N is known. Therefore, an attacker can try to compute the factorization of N. But up to now no algorithm is known that factors N in time polynomial in the bit-size of N.

In this work, we show that an attacker can determine the factorization of N in polynomial time, provided that e is of a special form or that the attacker gets into possession of a fraction of the secret key bits. The main method that we use in order to achieve our results is a method for finding small solutions of modular polynomial equations, which was proposed in 1996 by Coppersmith. Our main results in this dissertation thesis are:

- Generalization of Coppersmith's method for univariate polynomials. We also propose an approach for constructing optimal lattice bases, which are used in Coppersmith's method.

- Polynomial time factorization of N given (N, e), provided that the corresponding d is of the form $d = \frac{d_1}{d_2} \bmod (p-1)(q-1)$ for small d_1, d_2.

  This result leads to the crytanalysis of an RSA-variant that was proposed in 2001.

- Polynomial time factorization of N, provided that the parameter $d_p = d \bmod p - 1$ is small and that $q \leq N^{0.382}$. Small values of d_p are often used in practice since they speed up the decryption process.

- Several polynomial time attacks on RSA, provided that a fraction of the bits of d or of d_p is known. These attacks are also generalized to RSA moduli of the form $N = p^r q$ for $r > 1$.