The art of cryptography, summer 2013

Lattices and cryptography

Prof. Dr. Joachim von zur Gathen

Consider the Chinese Remainder version CRT-RSA of RSA, where the $n/2$-bit prime factors p and q of N are kept as part of the secret key. The exponents d and e are reduced modulo $p-1$ and $q-1$, respectively, to obtain d_p, d_q, e_p, and e_q. Then the RSA exponentiation can be performed with only one eighth of the cost of the standard method.
How many bits of the $n/2$-bit d_q are sufficient? We show that slightly more than the top half are enough, provided that the public exponent e is small.

LEMMA 1. *Let* $p, q, N = pq$ *be as in the RSA notation,* k *and* v *positive integers with* $k \neq 0$ *in* $\mathbb{Z}_p$ *and*

$$|kq - v| \leq N^{1/4}.$$

Given N *and* v*, we can compute* q *in polynomial time.*

THEOREM 2. *In the RSA notation p, q, N, e, d, assume that $N^{1/4} < p < q$ and $1 < e \leq N^{\alpha}$ for some α with $0 < \alpha \leq 1/4$, and let $v \in \mathbb{Z}$ be an approximation of $d_q \in \mathbb{Z}_{q-1}$ with*

$$|d_q - v| \leq N^{1/4-\alpha}.$$

Given N and v, one can factor N in polynomial time.

Corollary 3. *As in Theorem 3, we take the RSA notation* $p, q, N, d, e,$ *and* $0 < \alpha \leq 1/4$ *with* $N^{1/4} < p < q$ *and* $1 < e \leq N^{\alpha}$*, and assume that* N *is hard to factor. Then it is hard to find an approximation to* d_q *to within* $N^{1/4-\alpha}$*.*

EXAMPLE 4. Parts of the German online banking system used a 1024-bit RSA modulus N, between 2^{1023} and 2^{1024}, and a fixed public exponent $e = 2^{16} + 1 = 65\,337 = 2^{1024/64} + 1$. For each such N, we have $2^{16} + 1 \leq N^{\alpha}$ with $\alpha < 0.016$. We can apply the corollary and conclude that it is hard to approximate d_q to within $N^{1/4-\alpha} > 2^{239.7}$.

If d is sufficiently random, then d_q is likely to have about 512 bits. If we assume N to be hard to factor, then it is hard to find the top $512 - 239 = 273$ bits of d_q.