(Very) Large RSA Private Exponent Vulnerabilities

M. Jason Hinek
School of Computer Science, University of Waterloo
Waterloo, Ontario, N2L-3G1, Canada
mjhinek@alumni.uwaterloo.ca

February 2, 2004

Abstract

The dangers of using RSA with small private exponents has been known for more than a decade (see Wiener [7]). Knowing these dangers, but still wanting to substantially decrease decryption time, a user might try using a small negative private exponent which corresponds to a very large private exponent. We show that the attacks against small private exponent RSA by Wiener [7], Boneh & Durfee [3], and Blömer & May [1], and their corresponding attacks on multi-prime RSA, also work for very large private exponents.

1 Introduction

It is common to think that all RSA computations are performed in the positive representation (i.e., all values are always positive). If the public and private exponents are in the symmetric representation, however, the computational cost of exponentiation can be substantially reduced by using small negative exponents. In fact, if d is a small positive exponent then the cost of computing m^{-d} modulo N is simply the cost of computing m^d modulo N plus one inversion modulo N.

Knowing the dangers of using small positive private RSA exponents a user may be temped to use a small negative private exponent in order to speed up the time for decryption. In the next few sections, we will show that using small negative private exponents is just as dangerous as using small positive private exponents in RSA and multi-prime RSA.

Before considering the dangers of using very large private exponents we consider another simple observation that arises when thinking in the symmetric representation rather than the positive representation. Consider RSA with public exponent $e = 3$. An obvious weakness of textbook RSA without random padding is that ciphertexts corresponding to very small plaintext messages, $0 < m < N^{1/3}$, can be decrypted by simply computing the cube root of

$c = m^3 \bmod N$ over the integers. This works, of course, since $m^3 < N$. Similarly, ciphertexts of very large plaintexts can be decrypted too. Consider any plaintext in the range $N - N^{1/3} < m < N$. In the symmetric representation, this corresponds to $-N^{1/3} < m < 0$. Letting $c = m^3 \bmod N$, we can recover the plaintext by simply negating the cube root of $-c \bmod N$ over the integers. That is, $m = -\sqrt[3]{-c}$, where the cube root computation is over the integers, but everything else is reduced modulo N.

2 Continued Fraction Attack

Wiener's continued fraction attack on small private exponent RSA [7] is easily extended to very large private exponent RSA.

Theorem 1. *Let N be an RSA modulus with balanced primes and let d be a private exponent satisfying $\sqrt{6}\,(\phi(N) - d) < N^{1/4}$. Given the public key, (N, e), the private exponent can be recovered in time polynomial in $\log_2 N$.*

The proof is essentially the same as that given by Boneh in [2], and relies on the following facts.

Fact 1 (Hardy-Wright [5]). *Let a, b be integers and x a real number. If $|a/b - x| < 1/(2b^2)$ then a/b is a convergent of x.*

Fact 2 (Balanced Primes). *Let $N = pq$ be an RSA modulus where the primes satisfy $4 < \frac{1}{2}N^{1/2} < p < N^{1/2} < q < 2N^{1/2}$. Then, Euler's totient function evaluated at N satisfies $N - \phi(N) < 3N^{1/2} - 1$. These primes are called balanced primes.*

Proof. Proof (Theorem 1) By construction, we know $ed \equiv 1 \pmod{\phi(N)}$ which is equivalent to $e(d - \phi(N)) \equiv 1 \pmod{\phi(N)}$. Letting $D = \phi(N) - d$, we can write this as

$$eD = -1 + k\phi(N), \tag{1}$$

for some positive integer $k < D$. The bound on k is due to e being bounded above by $\phi(N)$. Using equation (1), Fact 2, $k > 1$, and $\sqrt{6}D < N^{1/4}$ we see that

$$\left|\frac{e}{N} - \frac{k}{D}\right| = \left|\frac{eD - kN}{ND}\right| = \left|\frac{(-1 + k\phi(N)) - kN}{ND}\right| = \left|\frac{1 + k(N - \phi(N))}{ND}\right|$$
$$\leq \frac{1 + k(3N^{1/2} - 1)}{ND} \leq \frac{k}{ND} 3N^{1/2} \leq \frac{3}{N^{1/2}} < \frac{1}{2D^2}.$$

Therefore, by Fact 1, k/D is a convergent of e/N. Using the continued fraction algorithm we can compute all the convergents of e/N and test for the correct k/D. Let k'/D' be a given convergent of e/N. Since k'/D' and k/D are in their lowest terms (property of continued fraction algorithm and $\gcd(k, D) = 1$, respectively) we can compute $\phi' = (eD' + 1)/k'$ and try to factor N. When $k'/D' = k/D$ we have $\phi' = \phi(N)$ and the factorization of N will be obtained.

Having factored N, we compute compute $d = e^{-1} \pmod{\phi(N)}$. Of course, $d = \phi(N) - D$ also. Since there are at most $\log_2(N)$ convergents of e/N and all arithmetic is done with numbers bound by N the result follows. □

Some experimental results of Weiner's continued fraction attack against large private exponent is shown below in Figure 1.

δ ($d = -N^\delta$)	0.01	0.05	0.10	0.15	0.20	0.25
convergent	10	28	66	86	118	150

Figure 1: Weiner's continued fraction attack against RSA with very large private exponent. A different 1024-bit modulus was used for each trial. The top row shows the size of d in the symmetric representation with respect to N. The bottom row shows the number of convergents needed to recover k/D.

3 The Small Inverse Attacks

The small private exponent attacks of Boneh & Durfee [3] are based on solving the so-called small inverse problem. That is, given integers A and M find an x_0 and y_0 such that $x_0(A + y_0) \equiv 1 \pmod{M}$, where x_0 and y_0 are small (in some sense). In particular, for RSA, let $e = N^\alpha$ with $\alpha \approx 1$, $d < N^\delta$, and $f(x, y) = x(N + y) - 1$. We then wish to find x_0 and y_0 such that

$$f(x_0, y_0) \equiv 0 \pmod{e} \quad , \quad |x_0| < X = N^\delta \quad , \quad |y_0| < Y = 3N^{1/2}. \tag{2}$$

One solution of (2) is $(x_0, y_0) = (k, \phi(N) - N)$, where k is the positive integer defined by $ed - k\phi(N) = 1$. Finding this solution reveals $\phi(N)$ and so the private exponent can be computed as $d = e^{-1} \pmod{\phi(N)}$. In [3], Boneh & Durfee present attacks that find the desired solution of (2) provided that $d < N^{0.284}$ or $d < N^{0.292}$. Another attack, by Blömer & May [1], finds the desired solution provided $d < N^{0.290}$. All of these results are asymptotic in the size of N and the dimension of the lattice used in the attack. We leave the details of the actual attacks to [3] and [1]. Also, as these attacks use Coppersmith's method of finding small roots of bivariate modular polynomials they are only heuristic. In practise they seem to work quite well though. Each of these attacks also work for very large private exponents as well.

Theorem 2. *For each attack against small private exponent RSA based on solving the small inverse problem in [3] and [1], if the attack works for all $d < N^\delta$ for some δ then the attack also works all $d > \phi(N) - N^\delta$.*

In the proof of this theorem, we only consider the $\alpha \approx 1$ case as this simplifies the bounds on X and Y. The more general case is essentially identical except that the bounds are slightly more complicated as they explicitly depend on α.

Proof. Proof (Theorem 2) By construction, we know $ed \equiv 1 \pmod{\phi(N)}$ which is equivalent to $e(d - \phi(N)) \equiv 1 \pmod{\phi(N)}$. This can be written as

$$e(d - \phi(N)) = 1 - \kappa\phi(N), \tag{3}$$

where κ is a positive integer. Since $e < \phi(N)$ we have that $\kappa < |d - \phi(N)| < N^{\delta}$. Letting $\phi(N) = N - \Lambda$ and reducing equation (1) modulo e gives

$$\kappa(N - \Lambda) \equiv 1 \pmod{e}, \tag{4}$$

where $|\kappa| < N^{\delta}$ and, by Fact 2, $|\Lambda| < 3N^{1/2}$. But, this is exactly the same starting point as in the attacks of Boneh & Durfee [3] and Blömer & May [1]. The correctness of their attacks finishes this proof. □

To illustrate the attack on small negative private exponent RSA, we used Boneh & Durfee's attack for $d < N^{0.284}$ and Blömer & May's attack for $d < N^{0.290}$ on RSA with a 1024-bit modulus and private exponent $d = -N^{0.265}$. Figure 2 shows the lattice dimensions and time required for the successful attacks.

Method	Lat. Dim.	m	t	Time (sec)
Boneh & Durfee	33	5	2	177 / 56
Blömer & May	18	5	2	77 / 70

Figure 2: Small private exponent attacks on RSA with 1024-bit modulus and private exponent $d = -N^{0.265}$. The parameters m and t define the lattice used in the attack. The last column shows the time needed for the attack. The time needed for lattice reduction (first) and resultant computations (second) are given.

4 Multi-prime RSA

In [6], Hinek, Low, and Teske extend most of the small private exponent attacks against RSA to multi-prime RSA. The only attack not extended is Boneh & Durfee's attack using geometrically progressive matrices (see [3]) that give the $d < N^{0.292}$ bound. This attack, however, was extended to multi-prime RSA for the $\alpha \approx 1$ case in [4] by Ciet *et al.* All of these attacks that have been extended to multi-prime RSA, just as with RSA, also work with very large private exponent.

Theorem 3. *Let N be an r-prime RSA modulus with balanced primes and let d be a private exponent satisfying $\sqrt{2(2r-1)}\,|\phi(N) - d| < N^{1/(2r)}$. Given the public key, (N, e), with non-negligible probability the private exponent can be recovered in time polynomial in the size of N.*

The proof of this result relies Fact 1 and on the following bound on $N - \phi(N)$ for balanced primes when the modulus has more than 2 primes.

Fact 3 (Balanced Primes). *Let* $N = \prod_{i=1}^{r} p_i$ *be the product of* r *prime numbers satisfying* $p_i < p_{i+1}$ *and* $4 < \frac{1}{2}N^{1/2} < p_1 < N^{1/r} < p_r < 2N^{1/r}$. *Then, Euler's totient function evaluated at* N *satisfies* $N - \phi(N) < (2r-1)N^{1-1/r} - 1$. *These primes are called balanced primes.*

Proof. Sketch Proof (Theorem 3) The proof is essentially the same as that for Theorem 1 except that we can no longer deterministically factor the modulus given $\phi(N)$. For $r = 3$ or 4, a probabilistic method for factoring N given a multiple of $\phi(N)$ is given by Hinek, Low, and Teske [6]. Alternatively, one can use a different test for each convergent. Let k'/D' be a given convergent of e/N. Since k'/D' and k/D are in their lowest terms we know D'. And, by definition of D ($D = \phi(N) - d$), we know that $-eD \equiv 1 \pmod{\phi(N)}$. So, for random $0 < m < N$ we can test if $m \equiv m^{-eD'} \pmod{N}$. If $m \not\equiv m^{-eD'} \pmod{N}$ we know $D' \neq D$ and try another convergent. If $m \equiv m^{-eD'} \pmod{N}$ for several values of m it is very likely that $-eD \equiv 1 \pmod{\phi(N)}$ and so we have found the private exponent in symmetric representation. For the positive representation we then compute $d' = \phi' - D'$ where $\phi' = (eD' + 1)/k'$. □

Theorem 4. *For each attack against small private exponent multi-prime RSA based on solving the small inverse problem in [6] and [4], if the attack works for all* $d < N^{\delta}$ *for some* δ *then the attack also works all* $d > \phi(N) - N^{\delta}$.

The proof follows from the proof of Theorem 2.

5 Conclusions

By simply considering the private exponent in the symmetric representation modulo $\phi(N)$ we have shown that very large private exponents are just as unsafe as small private exponents. In particular, for RSA, it is provably unsafe to use any private exponent $|d| < N^{1/4}/\sqrt{6}$ and heuristically unsafe to use any private exponent $|d| < N^{0.292}$.

References

[1] J. Blömer and A. May. Low secret exponent RSA revisited. In *Cryptography and Lattices – Proceedings of CALC '01*, volume 2146 of *Lecture Notes In Computer Science*, pages 4–19. Springer-Verlag, 2001.

[2] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society (AMS)*, 46(2):203–213, 1999.

[3] D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^{0.292}$. *IEEE Transactions on Information Theory*, 46(4):1339–1349, July 2000.

[4] M. Ciet, F. Koeune, F. Laguillaumie, and J.-J. Quisquater. Short private exponent attacks on fast variants of rsa. UCL Crypto Group Technical Report Series CG-2003/4, Université Catholique de Louvain, 2003. Available at `http://www.dice.ucl.ac.be./crypto/tech_reports/CG2002_4.ps`.

[5] G. Hardy and E. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, third edition, 1956.

[6] M. J. Hinek, M. K. Low, and E. Teske. On some attacks on multi-prime rsa. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography*, volume 2595 of *Lecture Notes in Computer Science*, pages 385–404. Springer-Verlag, 2003. (SAC 2002 proceedings).

[7] M. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553–558, 1990.