On using Carmichael numbers for public key encryption systems

R.G.E. Pinch

Queens' College, Silver Street, Cambridge CB3 9ET, U.K.

Abstract. We show that the inadvertent use of a Carmichael number instead of a prime factor in the modulus of an RSA cryptosystem is likely to make the system fatally vulnerable, but that such numbers may be detected.

1 Introduction

Huthnance and Warndof [12] comment that if one of the factors of the modulus in an RSA cryptosystem [23] is a Carmichael number rather than a prime, the cryptosystem will still work as expected. In this note we show that for the currently popular choice of 512 bit moduli, this would bring the modulus within the range of the elliptic curve factoring method [15], and that the most probable Carmichael numbers which might arise from currently popular primality tests can be factored very quickly by the $p+1$ method [26].

2 Primality tests

Many primality tests in current use [18],[19] are based on some form of the Fermat criterion: P is composite unless $b^{P-1} \equiv 1 \bmod P$. A *Carmichael number* is a composite number which satisfies the Fermat condition for all b coprime to P: hence the Fermat test is no more likely to reveal compositeness in this case than trial division.

The Fermat condition can be strengthened at little extra computational cost to the "strong" or Miller–Rabin criterion: putting $P-1 = 2^r s$, with s odd, the sequence

$$b^s, b^{2s}, b^{2^2 s}, \ldots, b^{2^r s} = b^{P-1} \quad \bmod P$$

should end in 1 (the Fermat condition) and the last term which is not 1 (if any) should be $-1 \bmod P$. There are no analogues of Carmichael numbers for this test; indeed, for composite P the proportion of $b \bmod P$ for which the criterion holds is less than 1/4. In each case we refer to a composite number which passes the test as a *pseudoprime* for that test.

Version 2 of the popular PGP implementation [27],[28] of the RSA cryptosystem uses four rounds of the Fermat test, with $b = 2$, 3, 5 and 7, and declares a number prime if it passes all four tests. The RSA Inc. B/SAFE toolkit uses four rounds of the Miller–Rabin test [13] with bases $b = 3$, 5, 7 and 11.

The composite numbers most likely to satisfy these criteria, and hence be falsely accepted as primes were classified by Damgård, Landrock and Pomerance [7],[8]. They showed that the most likely class of composites to escape detection are Carmichael numbers with three prime factors.

Huthnance and Warndof observed that RSA encryption and decryption [12] can be regarded as an elaborate form of the Fermat test, and hence that if an RSA modulus is formed inadvertently using a Carmichael number instead of a prime factor, then the cryptosystem will still function correctly. They argue that it is therefore unnecessary to pursue any more elaborate primality tests.

We maintain in this paper that this is dangerous advice.

3 Carmichael numbers

We record from [17] that a Carmichael number N has the following properties: N is square-free; N has at least three prime factors; $p \mid N$ implies $p-1 \mid N-1$ and $p < \sqrt{N}$.

A simple method of generating Carmichael numbers is due to Chernick [6]. If the three factors in $N = (6k+1)(12k+1)(18k+1)$ are simultaneously prime, then N is a Carmichael number. It is not yet known whether there are infinitely many Carmichael numbers of Chernick form, although this would follow from the more general conjecture of Dickson [11].

We are interested in Carmichael numbers with three prime factors. Their distribution has been studied by Balasubramanian and Nagaraj [4], who show that the number of such Carmichael numbers up to x is at most $\mathrm{O}\bigl(x^{5/14+\epsilon}\bigr)$. If $N = pqr$ is a Carmichael number then we have $p-1 = ha$, $q-1 = hb$ and $r-1 = hc$ where a, b, c are coprime and $habc \mid N-1$. So h must satisfy the congruence $h(ab+bc+ca) \equiv -(a+b+c) \bmod abc$. The Chernick form is the case $a = 1$, $b = 2$, $c = 3$, leading to $h \equiv 0 \bmod 6$. We see that most values of (a, b, c) will lead to a possible congruence for $h \bmod abc$, whose smallest solution may be expected to be of the same order as abc.

Using the methods of [17] we have been able to compute the Carmichael numbers up to 10^{18} with three prime factors[1]. There are 35585 of them (compared with 24 739 954 287 740 860 primes: Deléglise and Rivat [9],[10]).

Of these 35585 Carmichael numbers, 783 correspond to the Chernick form with parameters $(a, b, c) = (1, 2, 3)$ and a total of 4091 have $(a, b) = (1, 2)$. There were no other cases with $b/a = 2$. We may expect small values of abc to predominate since in general we may expect h to about the same order as abc and thus N to be at least $(abc)^2$.

4 Detecting Carmichael numbers with three prime factors

Let us consider how to guard against the possiblity that a number P generated during the construction of an RSA modulus is composite: we consider especially the case of detecting Carmichael numbers.

We should point out that this event is somewhat unlikely. The exact computations for 18-digits numbers shows that Carmichael numbers are extremely rare compared to primes.

We can apply a primality proving method such as ECPP [3] or APR-CL [2] to P. Such methods are applicable in general and quite practical for numbers of hundreds of decimal digits.

We note that one prime factor of a Carmichael number P has to be less that $P^{1/3}$. For an RSA modulus of 512 bits, we can assume that P is about 2^{256} and so has a factor at most 2^{86}, about 10^{26}. Such factors may be routinely extracted by the elliptic curve factoring method (ECM) of Lenstra [15]. For a modulus of 1024 bits, the smallest factor of P could be over 50 digits and this is just beyond the present extreme of the ECM (47 digits in a 135-digit factor of $5^{256}+1$ by Montgomery in December 1995).

We note that Carmichael numbers of any fixed form, for example, with given values of (a, b, c) but unknown h can be detected quickly by solving a single equation in h as a real variable. We demonstrate in the next section that a Carmichael number with parameters satisfying $b/a = 2$ is also easy to detect, even as a factor.

[1] The tables are available at `ftp://ftp.dpmms.cam.ac.uk/pub/Carmichael`

5 Detecting numbers divisible by a Carmichael number

Let us suppose that N is an RSA modulus divisible by a pseudoprime P. It is likely that P is a Carmichael number with three prime factors, say $P = pqr$; and again likely that the parameters (a, b, c) are all small.

Let us concentrate on the case $b = 2a$: for example, $a = 1$, $b = 2$. We saw that this occurred in over 10% of such numbers up to 10^{18}. We have $p = 2g+1$, $q = 4g+1$ for some g, so that $q + 1 = 2p$. So $2N$ is a multiple of $q + 1$, and hence q can be extracted immediately by the $p + 1$ factoring method of Williams [26]. Knowledge of q immediately yields g and hence p. We finally need to extract r. If N is 512 bits long then N/pq will be at most 100 digits and so can be factored by general purpose methods. Since r is congruent to 1 modulo a factor of g which is probably g itself, one could also use the Brent–Pollard modification [5] of Pollard's rho method [20],[21] for finding factors in given congruence classes.

6 Rare events and standards

Rivest [22] described numerical experiments using probabilistic primality tests for finding primes for potential use in an RSA cryptosystem and concluded that in practice the probability of obtaining a composite number was within acceptable limits. The estimates of Damgård, Landrock and Pomerance [7],[8] show that for the size of primes likely to be used in practice the probability of inadvertently finding a composite number is negligible (less than 2^{-100}, say). Some authors, such as Landrock [14] and Silverman [25] have concluded that there is no point in including requirements for primality proofs in standards such as ANSI X9.31.

We suggest that such requirements are not pointless. If an RSA cryptosystem is being used to sign digital documents, it may be to the advantage of a user to deliberately weaken his published modulus in order to subsequently repudiate a document, which he has in fact signed, by asserting that the weakness arose by chance and that an intruder has discovered the weakness. (Such a situation might arise, for example, in the context of electronic share trading.) Imposing checks against such weaknesses in the standard immediately eliminates this possibility, and avoids the necessity for contesting the plausibility of such claims in court.

7 Conclusion

Reliance on a probabilistic primality test for construction of an RSA modulus is likely to lead to a choice of factors which if not prime leave the system fatally weak. Proving the primality of the factors is reasonably fast, guards against an admittedly unlikely event and can prevent some forms of cheating.

References

1. L.M. Adleman and M.-D.A. Huang (eds.), *Algorithmic number theory*, Lecture notes in Computer Science, vol. 877, Berlin, Springer–Verlag, 1994, Proceedings, first international symposium, Ithaca, NY, May 1994.
2. L.M. Adleman, C. Pomerance, and R. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. **17** (1983), 173–206.
3. A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68, Lehmer memorial issue.
4. R. Balasubramanian and S.V. Nagaraj, *Density of Carmichael numbers with three prime factors*, Math. Comp. **66** (1997), no. 220, 1705–1708.

5. R.P. Brent and J.M. Pollard, *Factorization of the eighth Fermat number*, Math. Comp. **36** (1981), no. 154, 627–630.
6. J. Chernick, *On Fermat's simple theorem*, Bull. Amer. Math. Soc. **45** (1939), 269–274.
7. I. Damgård and P. Landrock, *Improved bounds for the Rabin primality test*, Cryptography and coding III (M. Ganley, ed.), IMA conference series (n.s.), vol. 45, Institute of Mathematics and its Applications, Oxford University Press, 1993, Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 117–128.
8. I. Damgård, P. Landrock, and C. Pomerance, *Average case error estimates for the strong probable prime test*, Math. Comp. **61** (1993), 177–194, Lehmer memorial issue.
9. M. Deléglise and J. Rivat, *Computing $\pi(x)$, $M(x)$ and $\Psi(x)$*, In Adleman and Huang [1], Proceedings, first international symposium, Ithaca, NY, May 1994, p. 264.
10. ———, *Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method*, Math. Comp. **65** (1996), no. 213, 235–245.
11. L.E. Dickson, *A new extension of dirichlet's theorem on prime numbers*, Messenger of Mathematics **33** (1904), 155–161.
12. E.D. Huthnance and J. Warndof, *On using primes for public key encryption systems*, Appl. Math. Lett. **1** (1988), no. 3, 225–227.
13. B.S. Kaliski jr, *How RSA's toolkits generate primes*, Tech. Report 003-903028-100-000-000, RSA Laboratories, Redwood City, CA, 18 Feb 1994.
14. P. Landrock, *Proper key generation*, Cryptomathic Bull. **1** (1996), at URL `http://www.cryptomathic.dk/m̃att/news.html`.
15. H.W. Lenstra jr, *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673.
16. A.J. Menezes and S.A. Vanstone (eds.), *Advances in cryptology —* CRYPTO *'90*, Lecture notes in Computer Science, vol. 537, Berlin, Springer–Verlag, 1991.
17. R.G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.
18. ———, *Some primality testing algorithms*, Notices Amer. Math. Soc. **40** (1993), no. 9, 1203–1210.
19. ———, *Some primality testing algorithms*, The Rhine workshop on computer algebra, Karlsruhe, March, 1994 proceedings (J. Calmet, ed.), February 1994, pp. 2–13.
20. J.M. Pollard, *Theorems on factorization and primality testing*, Proc. Cambridge Philos. Soc. **76** (1974), 521–528.
21. ———, *A Monte Carlo method for factorization*, BIT **15** (1975), 331–334.
22. R.L. Rivest, *Finding four million large random primes*, In Menezes and Vanstone [16], pp. 625–626.
23. R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **21** (1978), no. 2, 120–126, Reprinted as [24].
24. ———, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM **26** (1983), no. 1, 96–99, Reprint of [23].
25. R.D. Silverman, *Fast generation of random, strong RSA primes*, Cryptobytes **3** (1997), no. 1, 9–13.
26. H.C. Williams, *A $p+1$ method of factoring*, Math. Comp. **39** (1982), 225–234.
27. P.R. Zimmerman, *The official PGP user's guide*, MIT Press, 1995, 0-262-74017-6.
28. ———, *PGP source code and internals*, MIT Press, 1995.