CRYPTANALYSIS OF SHORT RSA SECRET EXPONENTS

Michael J. Wiener

Bell-Northern Research Ltd.
P.O. Box 3511 Station C
Ottawa, Ontario, Canada K1Y 4H7

Abstract[1]

A cryptanalytic attack on the use of short RSA secret exponents is described. This attack makes use of an algorithm based on continued fractions that finds the numerator and the denominator of a fraction in polynomial time when a close enough estimate of the fraction is known. The public exponent e and the modulus pq can be used to create an estimate of a fraction that involves the secret exponent d. The algorithm based on continued fractions uses this estimate to discover sufficiently short secret exponents. For a typical case where $e < pq$, $\gcd(p-1, q-1)$ is small, and p and q have approximately the same number of bits, this attack will discover secret exponents with up to approximately one-quarter as many bits as the modulus. Ways to combat this attack, ways to improve it, and two open problems are described. This attack poses no threat to normal case RSA where the secret exponent is approximately the same size as the modulus. This is because this attack uses information provided by the public exponent and, in the normal case, the public exponent can be chosen almost independently of the modulus.

[1]For the full paper, the reader is referred to the IEEE Transactions on Information Theory, Vol. 36, No. 3, May 1990, p. 553-558.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, p. 372, 1990.