Twin RSA

Arjen K. Lenstra[1,2] and Benjamin M.M. de Weger[2]

[1] Lucent Technologies, Bell Laboratories, Room 2T-504,
600 Mountain Avenue, P.O.Box 636, Murray Hill, NJ 07974-0636, USA
[2] Technische Universiteit Eindhoven,
P.O.Box 513, 5600 MB Eindhoven, The Netherlands

Abstract. We introduce *Twin RSA*, pairs of RSA moduli $(n, n+2)$, and formulate several questions related to it. Our main questions are: is Twin RSA secure, and what is it good for?

Keywords: recreational cryptography.

1 Introduction

Regular RSA moduli are constructed by multiplying two more or less randomly selected primes of appropriate sizes. As a result, representation of a regular $2N$-bit RSA modulus requires about $2N$ bits. To save on the representation size of RSA moduli, several methods were proposed in [8], some of which were broken in [1]. An often reinvented folklore approach to generate $2N$-bit RSA moduli that can be represented using just N bits, published in [5] along with several simple variants, still seems to be unbroken. This simple method works as follows. For an N-bit number x that is known from the context, repeatedly select an N-bit prime p at random until the integer part q of the quotient $(x+1)2^N/p$ is prime, then the most significant N bits of the RSA modulus $n = pq$ are given by x. Faster variants add some slack to x and replace q by $q+1$ until it is prime, but the principle remains the same. Since x is known from the context—or can for instance be chosen as 2^{N-1}—the N least significant bits suffice to represent the $2N$-bit RSA modulus n. If one is willing to also consider moduli of unbalanced factor sizes, e.g. a product of primes of sizes $\frac{1}{2}N$ and $\frac{3}{2}N$, respectively, then, as was shown in [5], a $2N$-bit modulus can even be represented using $\frac{1}{2}N$ bits. In particular this shows that pairs of RSA moduli can be generated in such a way that the pair can be represented using the space of a single regular or even a half unbalanced RSA modulus.

In this note we present a method that achieves the same 'compression ratio' for pairs of RSA moduli, in a different and esthetically more pleasing way. Our method is implicit in one of the methods described in [6] and thus not new. The reason we present this particular case of the method from [6] is the fact that the possibility of the construction is usually met first with amazement, quickly followed by skepticism about the security, and finally with puzzled resignation that the resulting moduli indeed look hard to break. Thus, we would like to

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 222–228, 2005.

offer it as a challenge to a wider audience, hoping for either a better security argument than what can be found in [6], or a more effective cryptanalysis.

Another question we want to pose with this note is: are there any applications of Twin RSA that are more interesting than the ones we have been able to offer so far? We realize that it is by no means good marketing policy to present a new cryptographic method without convincing evidence of its practical potential or cryptographic significance. On the other hand, publishing the method despite the fact that we cannot think of a sensible application ourselves, at least has the potential to uncover new possibilities by bringing it to the attention of members of the practical cryptographic community who may never have realized that such remarkable pairs of RSA moduli were possible—or secure.

The remainder of this note is organized as follows. Our method to generate RSA moduli with a fixed prescribed difference is described and discussed in Section 2. A few generalizations are offered in Section 3, and Section 4 concludes this note with two factoring challenges.

2 Twin RSA

Generation of RSA moduli with any prescribed even integer difference d is an easy application of the Chinese Remainder Theorem. The details are described in Algorithm 1 below.

Algorithm 1. Let $d \neq 0$ be a small fixed even integer and let $2N$ be the bitlength of the RSA moduli to be generated.

1. Select two random N-bit primes p and q.
2. Use the Chinese Remainder Theorem to calculate the least positive integer n such that $n \equiv 0 \bmod p$ and $n \equiv -d \bmod q$ and let $r = n/p$ and $s = (n+d)/q$.
3. If n or $n + d$ does not have bitlength $2N$, or if r or s is composite, then return to Step 1.
4. Output the pair of RSA moduli $(n, n + d)$ with factorizations $n = pr$ and $n + d = qs$.

For actual RSA applications of the resulting moduli, co-primality requirements with respect to one's favorite public exponent(s) and $p-1$, $q-1$, $r-1$, and $s-1$ have to be included in the above description.

Twin RSA. We introduce the term *Twin RSA* for the pair of moduli that results from Algorithm 1 when $d = \pm 2$.

Abundance. A single moment of reflection learns that it is most likely the case that Twin RSA moduli are abundant. The Prime Number Theorem combined with the assumption that the factorizations of n and $n+2$ are independent leads to the conjecture that the number of Twin RSA moduli up to x is asymptotically equal to $cx/(\log x)^4$, for some positive constant c. The same argument applies to the general case $(n, n + d)$ for odd d.

Runtime of Algorithm 1. Based on the Prime Number Theorem and the runtime of a single probabilistic compositeness test (using standard arithmetic),