CORR 2002-11

On Some Attacks on Multi-Prime RSA

M. Jason Hinek, Mo King Low, & Edlyn Teske

Abstract Using more than two factors in the modulus of the RSA cryptosystem has the arithmetic advantage that the private key computations can be speeded up using Chinese remaindering. At the same time, with a proper choice of parameters, on does not have to work with a larger modulus to achieve the same level of security in terms of the difficulty of the integer factorization problem. However, numerous attacks on specific instances on the RSA cryptosystem are known that apply if, for example, the decryption or encryption exponent are chosen too small, or if partial knowledge of the private key is available. Little work is known on how such attacks perform in the multi-prime case. It turns out that most of these attacks it is crucial that the modulus contains exactly two primes. They become much less effective, or fail, when the modulus factors into more than two distinct primes.