H-Online.com

Researchers have decomposed a 768-bit number with 232 decimal places into its two prime factors and published a paper with their results . The number is the string released as ˝RSA-768˝ under the now defunct RSA Challenge . As a result, RSA encryptions with 768-bit keys must, from now on, be considered cracked.

It took the team of researchers from Switzerland, Japan, Germany, France, the US and the Netherlands about two and a half years to perform the factorisation. The first step of the calculation, polynomial selection, required half a year on a cluster consisting of 80 PCs, while the second and considerably more labour-intensive sieving step took about two years on a cluster of several hundred computers. According to the researchers, a single Opteron processor with 2 Gbytes of RAM would have needed about 1,500 years to complete the sieving step.

As RSA-512 was cracked about a decade ago, the researchers assume that the computing power required to master RSA-1024 is likely to become available in about ten years. They therefore recommend that all 1024-bit RSA keys be decommissioned by 2014 at the latest.