

Im Jahr 1994 wurden für die 129-Stellen Zahl "RSA129"

1143816257578888676692357799761466120102182
9672124236256256184293570693524573389783059
7123563958705058989075147599290026879543541

die Faktoren

3490529510847650949147849619903898133417764
638493387843990820577

und

3276913299326670954996198819083446141317764
22967992942539798288533

mit einem Aufwand von 5000 MIPS-Jahren [10^{18} Schritte] in einem weltweiten Netzwerk von 1600 Arbeitsplatzrechnern gefunden.

Mit derzeitiger Technologie bedarf es etwa 3 Milliarden MIPS-Jahre um eine Zahl mit 200 Stellen zu faktorisieren. No way!

Mit **Shor's Quantenalgorithmus** wäre man nach hundert Milliarden Schritten fertig ... wenn man einen **Quantencomputer** mit ca. 10000 Quantenbits hätte.