The RSA-155 Challenge

Challenge: Factor the following 155 digit (= 512 bit) number:

$$n = 109417386415705274218097073220403576120\\037329454492059909138421314763499842889\\347847179972578912673324976257528997818\\337970765372440271467435315933543338 97$$

Solution: (S. Cavallar, B. Dodson, A.K. Lenstra, B. Murphy, P.L. Montgomery, H.J.J te Riele; August, 1999)

By using the so-called Number Field Sieve one obtains that $n = pq$ with

$$p = 102639592829741105772054196573991675900\\716567808038066803341933521790711307779$$

$$q = 106603488380168454820927220360012878679\\207958575989291522270608237193062808643$$

Time estimate: The above factorization takes:

20 years on 1 PC = 1 day on 7500 PC's

Here: "PC" means a machine having 64MB memory and using 450MHz Pentium II processor (1999 standard).

Conclusion: RSA with a 155 digit modulus cannot be considered to be secure (even in 1999!)

The RSA-768 Challenge

Challenge: Factor the following 232 digit (= 768 bit) number:

$$n = 123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3$$

Solution: (T. Keinjung, K.Aoki, J. Franke, A.K. Lenstra, E. Thomé, P. Gaudry, E. Kruppa, P. Montgomery, J. Bos, D. Osvik, H. te Riele, A, Timofeev,P. Zimmermann; Dec., 2009) By using the so-called Number Field Sieve one obtains that $n = pq$ with

$$p = 33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489$$

$$q = 36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917$$

Time estimate: The above factorization took 2 years on a collection of parallel computers. The CPU time is equivalent to

2000 years on 1 PC

Here: "PC" means a machine using a single core 2.2GHz AMD processor.

Recommended Bit Sizes: A.K.Lenstra and E.R.Verheul proposed in Sep. 1999 the following minimum key sizes (in bits):

	2000	2005	2010	2025	2050
RSA	952	1149	1369	2174	4047
ECC	132	147	160	202	272