Primality Testing (polyn!!) vs Factoring (NPhard?) **[Spring 2006]**

Largest **randomly chosen** number **proven prime:** 15071-digits, July 2004

(Morain, Franke, Kleinjung, et.al.; 700 cpudays, 2.6 GHz xeon)
[distributed, ECPP]

Largest **cryptographic number** factored: 200-digits (662.5-bits), May 2005

RSA200 = (100-digit prime) * (100-digit prime)

(Franke, Kleinjung, et.al.; **sieving:** 55-cpuyears, 2.2 GHz Opteron [distributed];

matrix: $64M^2$, 171.87 1's/row, 3 months on cluster of 80 2.2 GHz Opt.
[Gigabit network]. GNFS)