Primality Testing (polyn?) vs Factoring (NPhard?) **[Spring 2000]**

Largest randomly chosen number proven prime: 1500-digits

Largest cryptographic number factored: 155-digits (512-bits)

RSA155 = (78-digit prime) * (78-digit prime)

(Cavallar, Dodson, Lenstra, Montgomery, et.al.,

found Aug 22, 1999, appeared EuroCrypt 2000, May.)