The RSA-155 Challenge

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

\[ n = 109417386415705274218097073220403576120 \\
03732945492059909138421314763499842889 \\
347847179972578912673324976257528997818 \\
3379707653724402714674353159335433897 \]

**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!)

**Recommended Bit Sizes:** A.K.Lenstra, E.R.Verheul (Sep. 1999)

<table>
<thead>
<tr>
<th></th>
<th>2000</th>
<th>2005</th>
<th>2010</th>
<th>2025</th>
<th>2050</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>952</td>
<td>1149</td>
<td>1369</td>
<td>2174</td>
<td>4047</td>
</tr>
<tr>
<td>ECC</td>
<td>132</td>
<td>147</td>
<td>160</td>
<td>202</td>
<td>272</td>
</tr>
</tbody>
</table>