Puzzle

May 14, 2018

TechWorm has a story entitled "Two Security Researchers Break RSA 4096 Bit Keys with 'Phuctor' " They did so by finding a common factor of the (different) moduli of two public keys. As these factors p and q are generated randomly, and are on the order of 2096 bits big, why might two of these factors be the same even when they are generated on two, often geographically widely separated, systems?

The URL of this story is:
`http://www.techworm.net/2015/05/two-security-researchers-break-rsa-4096-bit-keys-with-phuctor.html`