Prime Numbers and “safety” notes:

* As far as the best mathematicians and computer scientists have been able to determine, it is totally impossible to come up with a truly efficient formula for factoring large numbers into primes.
* When trying to factor large numbers into primes, taking a simple algorithm to factor would take forever (even for a computer)
* So, there is a functional limit to the size of the numbers we can factor into primes, and this fact is absolutely essential to modern computer security. Anything that computers can easily do without being able to easily undo will be of interest to computer security.
* Modern encryption algorithms exploit the fact that we can easily take two large primes and multiply them together to get a new, super-large number, but that no computer yet created can take that super-large number and quickly figure out which two primes went into making it.
* Its infinite existence was known as early as Euclid over 2000 years ago, yet the prime number theorem, regarding the distribution of prime numbers, was only proven in 1896, following Bernhard Riemann’s study of its connection to the Riemann zeta function. There remain still numerous unsolved conjectures to this day.
* Two well-known types of prime pairs are, twin primes, where both p and p+2 are primes, and Sophie Germain (1776-1831) primes, where both p and 2p+1 are primes. Extending the concept of Sophie Germain prime pairs, a chain of nearly doubled primes is named after Allan Cunningham (1842-1928)

-------------------------------------------------------------------------------------------------------------------------------

* <https://psmag.com/news/prime-numbers-keep-our-information-safe>
* The first ingredient required for the algorithm are two large prime numbers. The larger the numbers, the safer the encryption.
* In fact, the new prime is so large that, at present, no conceivable technological advancement in computing speed could lead to a need to use it for cryptographic safety. It is even likely that the risks posed by the looming quantum computers wouldn't need such monster numbers to be made safe.