True Random Number Generator / Hardware Random Number Generators

* Existing random number generators can only generate random numbers at a very slow rate, very slow when compared with the speed at which most computers run.
* If one tries to increase the sampling rate of such RNGs then it can often lead to correlation between successive numbers.
* Some RNGs are biased to some range of values (i.e., the probability distribution is not uniform) and therefore the numbers produced cannot be called as truly random. Often, the remedy applied in such cases is to mix these numbers with the numbers from a Pseudo Random Number Generator (PRNG).
* The mixing of random numbers is usually carried out by XOR of the numbers to get the final random number. This is expected to help improve the entropy (average randomness of a single random number) of random numbers produced.
* Uses – Cryptography, stochastic resonance, genetic algorithms, Monte Carlo simulations, Surrogat data method, creation of lottery numbers, many others.