A Random Number Generator in Hardware

A hardware random number generator is different from a pseudo-random number generator - a pseudo random number generator approximates the assumed behaviour of a real hardware random number generator. Simple pseudo random number generators suffices for most applications. Sometimes they do not, however. These include demanding situations as generating cryptographic keys, generating lists of winners of lotteries, generating data selections for statistical research papers and so on.

When Not to Use a Pseudo Random Number Generator

Suppose we wish to encrypt a communications link with a cipher system. We wish to generate 365 independent daily keys, and we chose a pseudo random number generator to expand an initial seed to 365 different daily keys. We assume that the length of the initial seed is much less then the total length of the 365 keys.

In this situation we have modified our cipher system, no longer do we have 365 independent daily cipher keys but instead we have a single "Initial Seed". The main reason why the use of a pseudo random number generator is not recommended in this situation is that to maintain security we must have a pseudo random number generator whose cryptographic strength is much higher than the cryptographic strength of the cipher system. If this is the case we may chose, without loss of security, to expand the "Initial Seed" to the length of all transmitted messages and then replace the cipher system with a "One Time Pad"-cipher.

In a cryptographic environment the use of independent daily keys are recommended because if one key is stolen only one day of communication can be read by the enemy. To obtain this we need to generate 365 independent initial seeds for our pseudo random number generator... which we apparently cannot simplify by using yet another pseudo random number generator...

The fact hidden in the above story is that it is not possible to expand the amount of information contained in the "Initial Seed" by clever computing.

It is difficult or impossible to generate 365 independent daily keys with a pseudo random number generator. Generating 365 independent daily keys with a hardware random number generator, however, is not that difficult or expensive.

Additional information about the generation of good random numbers can be found in Randomness Recommendations for Security
(http://info.internet.isi.edu:80/in-notes/rfc/files/rfc1750.txt).
This paper briefly explains currently known methods of random number generation without special purpose hardware.

Can a Hardware Random Number Generator be Used for My Purposes?

Cryptographic and statistical applications are general and demanding. A hardware random number generator supporting these applications can directly or easily be used for most random selection problems. If a statistician is in need of true random numbers drawn from some specified distribution he can usually, often quite easily, convert a series of true random numbers to this distribution. If not, some problem or situation may be simulated and the random numbers obtained as observations from the simulation.

If a cryptographer needs some specific entity, such as a prime number with a specific security property, the possibility to at least be able to select the starting point for the search, in a true random way, is of great importance.

For a lottery applicatio we need, in addition to the use of a good hardware random number generator, cryptographic protection against bias intentionally introduced by some party. We also need TEMPEST protection of the computers and building to secure the lottery from possible remote influence by radio waves. All software must be inspected and validated on site, and then protected against unauthorised modification.