The dealing algorithm used by Duplimate

A good dealing (shuffling) algorithm should have at least the following features:
• The sequence should be long enough
• It should be encrypted
• It should be well known and tested.

The Duplimate shuffler uses RipEMD that has these features. The bit count is 2^160, i.e. we have a sequence of 2^160. There are less than 2^96 bridge deals available, which means that we have a sufficiently long series.

The algorithm is a cryptographic hash algorithm, which means that you cannot calculate the outcome of the algorithm even if you would know the internal state of the generator.

RipEMDI60 was originally a project sponsored by the European Union, developed in the Netherlands. It was first used for bridge hand generation as a DOS version where the seed was taken by the time it took for the operator to press on a

PC:s keyboard 40 times. Then came a Windows version where the Random factor came from reading the position of the mouse cursor at certain intervals. In the Duplimate version of BigDeal the speed of the operator is used as random factor.

The source code of the Duplimate program (written in C++) is property of Jannersten Forlag. Very few people have ever seen the code. Hacking and decompiling the program is of course possible, but by using an encrypted hard disk, and keeping the computer secured, security should not be a problem. The deal files that are generated by the Duplimate software are encrypted by default.

References
Research on Random number generation is done at many famous universities in the world. You can find an enormous amount of information about this on the Internet.

Chapters 1 and 2 of James E. Gentle: Random Number Generation and Monte Carlo Methods give a good start for studies of the subject.

Last revised August 2011