Dealing program **Big Deal**

During this Olympiad hands are being predealt using the new dealing program **Big Deal**. This program is offered to you free of charge.

**Why a new program?**
It has been noticed in the bridge community that using dealing programs sometimes identical sets occur. Writers of these programs usually blame the operators for making some sort of mistake and indeed human errors do occur, but the signals were strong that there was also something wrong with the programs.
Hans van Staveren has been thinking this over for some time. He found the mistake and to remedy it he developed a new program that is correct. Now we let him do the talking:

*I have put my ideas about dealing programs before Koos Vrieze, professor of mathematics at the University of Maastricht. He screened my ideas and Jeroen Kuipers (one of his graduate students) assisted in building the program. It is finished now and it works. It has been posted on the Internet for a year. In contrast to the habit of most authors my source code is public. Everybody can see what I have done and everybody can check whether it is correct. Many clever guys have screened the program for imperfections.*
*The Dutch Bridge Federation has been using it for a year as a test and no serious errors were found. What do I want with this program? Actually I want all people to scrap their old programs and start using this new one. I offer it for free and if necessary I will adapt the output format. There is nothing in it for me, except for the joy of creation, and perhaps a boost of my ego.*

***What went wrong previously?***
*You want the computer to generate random sets of hands. Most computers can come up with (at most) 32 bits of random information. That number is already dubious; it probably is closer to 20 bits. If we assume 32 bits than this means that there can be* $2^{32}$ *different sets of hands generated; this number is close to four billion. That seems like an awful lot, but it is not if one considers that the number of possible bridgehands is somewhere in between* $2^{95}$ *and* $2^{96}$*. For the first board you have four billion possibilities and for the second also. In a set of 20 boards eighty billion possibilities. Some calculations reveal that there are almost a million times a million times a million as many bridgehands. With a dealing program you want to improve the dealing by hand. If the program isn't even able to produce all possible bridgehands, can we say this is an improvement? Some experts think this omission is acceptable, I do not.*
*But having a seed of 32 bits is even worse for another reason. If we assume four billion possibilities, when do you think you will be plagued by duplicate sets? After two billion sets? No. Think about the so-called birthday paradox. If you have 366 people together the chance that two persons will have their birthday on the same day is 100%. How many people are necessary for a chance of 50% of a double birthday? It turns out you need 23 people. Just simple mathematics. It is called the birthday paradox, because your intuition tells you the number should be much greater. If we replace the number of possible birthdays by four billion, how many sets do we need before the chance of a double set becomes significant, say 50%? That is the square root of four billion or 65,000. In practice it is even worse, since you probably haven't got 32 bits of randomness. Probably it is closer to only 20 bits and then you only have one million starting possibilities. After only 1000 sets it goes wrong. And that is just what we register now.*
*There is yet a third problem, that no one seems to have noticed so far. Suppose you play a session somewhere, and you have played four boards. You enter them into your handheld*

*computer. It is conceivable that there could be software that generates the rest of the boards of the session for you. This software has not been made yet. Although it would cost effort and money, it is not inconceivable that it will be made someday.*

***What has been improved?***

*All problems stem from lack of randomness. The number of possible bridgehands is something in between $2^{95}$ and $2^{96}$. So you have to start with at least 96 bits randomness. I have extracted extra randomness from the time that elapses between two keystrokes. After about 30 keystrokes (6-8 seconds) I have collected with my program 160 bits. I like to assume a pessimistic scenario. I then have $2^{160}$ possible starting values. As a start I can produce all possible bridgehands. Every starting value leads to a random hand. Because I have more starting values then there are bridgehands, it is possible that no bridgehands corresponds to the value. The program simply produces a new value.*

*Of course I also suffer from the birthday paradox. I start getting troubles with double sets after $2^{80}$ sets. If you let all the people in the world produce a set every couple of minutes then you start getting troubles after six billion years. In that time our sun will be extinguished, so we should be able to deal with that.*

*I have also secured the program in such a way that it is impossible to generate the whole set out of a first few hands. For that I used cryptographic hashes. These cryptographic hashes are primarily used for electronic financial transactions. It is a kind of digital signature. Because of the huge interests, the whole world tries to crack these cryptographic hashes. Whole armies of bright scientists have shown that these hashes cannot be cracked. I used these codes in writing this program.*

So throw away your old program and switch to **Big Deal**. This program is offered to you free of charge. For the interested detailed technical information is available.