

Random Numbers

Random numbers are used in many computer applications, especially on the internet to keep secret data unreadable for unauthorized people. But how does a machine of which we know its actions are all determined generate random numbers?

Answering this question, I will introduce the three types of random numbers - pseudorandom, true and hybrid random numbers - and will explain where and how they are used. There will be two examples to discuss in detail: cryptography and the Monte-Carlo-Simulation that use random numbers in different ways, thus needing different types. With the example of One-Time-Pads I will introduce several terms from the field of cryptography like perfect security and also explain how quantum computers can realize this. Concluding with the Monte-Carlo-Simulation and the quality of random numbers we will reencounter Pi twice.