

largely unnoticed yet universal feature of contemporary society. Basic scientific research and the selection of winners in competitions both call for a ready supply of random numbers. But what are pseudo-random numbers, why do we need them, and what bearing does their generation have on the present question of chaos out of order? In passing, it should be noticed that genuinely random numbers can be produced using physical processes, such as radioactive decay. If this is so and if the real thing is available one might ask why we should bother with something which is second best. The answer is that pseudo-random numbers are almost as good and do not require any physical apparatus with all its costs and inconvenience.

It may help to begin by looking at some familiar things which serve to introduce the general idea. In some sense we are talking about what might be called 'contrived' accidents. Think first of the tables of figures published by National Statistical Offices. Narrowing it down, imagine we are looking at the populations of large cities in a big country such as the United States. One such figure might be 1,374,216. Not all of the digits have equal importance. The first 1 is the most important. It immediately gives us an idea of whether this is a big city or not; in this instance it is in the million or more bracket. The next most significant digit is the 3 in the second position. Knowing that the city population was in the region of 1.3 million would probably tell us most of what we want to know and it would certainly fix the size in relation to most other major cities. As we move along the sequence the digits become progressively less significant. Another way of putting the matter is to say that the information, conveyed by these successive digits, diminishes as we move along the sequence. The final 6 tells us very little indeed about the size of this city, or about its size in relation to other cities. In fact, it may not be accurate given the uncertainties of counting such things. If