Cryptography and Lava Lamps

It's not as easy as you might think to be truly random

You're familiar with random patterns. The sales of most of your products have a random element – you know it as noise, and it's what drives your safety stock levels. It's important to understand whether something is random in order to know whether it can be forecast. Like your sales.

However, randomness is not an easy concept to define – and meanings vary according to the context. The Cambridge Online Dictionary says: "happening, done or chosen by chance rather than according to a plan". In statistics, a random number is one drawn from a set of equally probable values and statistically independent from others in the series. Computer programmers and cryptographers tend to describe a random sequence as arbitrary, unpredictable and incapable of being compressed into a shorter series.

If it's hard to define, it's also extremely difficult to test for or prove randomness in a series of numbers. Something which appears random may actually have an underlying pattern; for example, a sequence of bits may make no sense unless you have the cryptographic key to decode the series into a message.

Although random series are increasingly necessary nowadays for encryption and security, generating them is not straightforward. Computers can only simulate randomness, as they can only follow programmed instructions and formulae. True random number generators usually base their series on natural phenomena, such as atmospheric noise or even the motion of oil in a lava lamp (see www.lavarand.org for random numbers and even random poetry) – slower to produce results than the simulations, but genuinely random.

So where does this leave us? Random numbers are difficult to define, challenging to test and complicated to generate. The problem is summed up by an old mathematician's joke: decades ago, when statisticians needed random numbers, they consulted huge tables which were ungainly and awkward to use. To save time and effort they decided to find the most random number in the world, and use that instead. And after considerable research, they found it: their proof showed that this number could not be greater than 17, and it must not be less than 17, and therefore it was 17. And perhaps that really is the answer – maybe we just need to rephrase the question...