

Random Numbers

Exercises

- What is a random number?
 - A random number is a number whose value appears to be chosen by chance
- Give some examples of when random numbers are useful to programmers
 - Allowing the program to make unpredictable decisions (games and simulations)
 - Creating keys and credentials which are difficult to guess (cryptography and authentication)

- Why is it not possible for software algorithms to produce true random numbers?
 - Software algorithms are based on mathematics and logic, which are deterministic
- What does "PRNG" mean?
 - Pseudo-random Random Number Generator - uses maths
- Describe briefly what a PRNG does
 - It calculates a sequence of numbers which appear to be random. The sequence repeats when exhausted

- In the context of random numbers, what is meant by the term "seed"?
 - A seed is a value which is used to initialize the sequence
 - Using a different seed will cause a different sequence to be generated

- What does "TRNG" mean?
 - True Random Number Generator - uses events in the physical world
- Give some examples of a TRNG
 - Data tables generated from radioactive decay, thermal noise etc
 - “Entropy” providers in the operating system - data generated from user activity, processor temperature fluctuations, etc
 - Hardware devices - generate data from radioactive decay, air pressure fluctuations, etc