**Randomized Algorithms**

Randomized Algorithms are algorithms that use a random number at least once in a decision.

The problem is that no computer can produce truly random numbers. It instead uses an algorithm to calculate a virtually random number by using variables that change to some degree. The result is usually called a “pseudorandom” number.

Theoretically we can reverse engineer any result we get from this calculation but practically we can make the variables so complex that this will be very difficult. One popular way of getting this changing variable is using the systems clock as this will change between runs. Although this can, theoretically, be the same on different runs it is so extremely unlikely that it is disregarded. The biggest problem with this method is if you want to get multiple random numbers after each other. Even with a fairly small unit of time the system clock may not have changed so you end up with the same random number twice (or even more times). What we want then is a sequence of random numbers that is independent of each other. For example: if we want a sequence random numbers ranging from 1 to 2 each number should have a 50% chance of becoming 1.