Pseudo-random Generator

A pseudorandom generator (PRG) is a deterministic algorithm that takes a short random seed as input and generates a long output sequence that appears random to any efficient adversary who does not know the seed.

Proof of the security of a PRG by reduction:

1. Assume that we have a PRG (G) that expands a random n-bit seed s into a longer m-bit sequence G(s), where $m > n$. We want to show that **G is secure.**
2. Let D be an efficient distinguisher that takes an m-bit string as input and outputs a bit, where $D(x) = 1$ if x is the output of G(s) for some random s, and $D(x) = 0$ otherwise. We want to show that the advantage of D in distinguishing G(s) from a random m-bit string is negligible, meaning that it is bounded by some negligible function $\varepsilon(n)$.
3. We can assume without loss of generality that D is deterministic, since if D is probabilistic, we can simply take the maximum probability over all possible random choices of D.
4. Let R be a truly random m-bit string. We can define a new distinguisher D' as follows: on input x, D' outputs D(x) if x is not equal to R, and outputs 1 otherwise. Note that D' is deterministic and makes at most one query to its input.
5. We can then define the advantage of D in distinguishing G(s) from R as follows.

$$|\Pr[D(G(s)) = 1] - \Pr[D(R) = 1]| = |\Pr[D'(G(s)) = 1] - \Pr[D'(R) = 1]|$$

where the second equality follows from the fact that D and D' differ only on one possible input, namely R.

6. Let $\varepsilon'(n)$ be the advantage of D' in distinguishing G(s) from R. Then we have:

   $$|\Pr[D(G(s)) = 1] - \Pr[D(R) = 1]| = |\Pr[D'(G(s)) = 1] - \Pr[D'(R) = 1]| \leq \varepsilon'(n)$$

   where the inequality follows from the fact that D' is a valid distinguisher for G(s) and R.

7. We can then conclude that the advantage of D in distinguishing G(s) from a random m-bit string is negligible, because $\varepsilon'(n)$ is negligible and we can choose R uniformly at random.
8. Therefore, **we have shown that if G is a secure PRG**, then no efficient distinguisher D can distinguish its output from a truly random string with non-negligible advantage.