Cryptography

Lecture 13 III 2013

Definition (**Negligible**) A function f is *negligible* if for every polynomial $p(\cdot)$ there exists an N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.

Definition (**Pseudorandom function**) Let $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ be an efficient, length-preserving, keyed function. We say that F is a *pseudorandom function* if for all probabilistic polynomial-time distinguishers D (statistical tests D), there exists a negligible function negl such that:

$$\left| P\left(D^{F_k(\cdot)}(1^n) = 1\right) - P\left(D^{f(\cdot)}(1^n) = 1\right) \right| \leq \mathsf{negl}(n),$$

where $k \leftarrow \{0,1\}^n$ is chosen uniformly at random and f is chosen uniformly at random from the set of functions mapping n-bit strings to n-bit strings.

.