Crypto

Preliminaries and notation

- $S \subseteq \{0,1\}^*$ defines set S as a finite subset of $\{0,1\}$ all finite-length strings.
- $x \in_R S$, R indicates x is chosen randomly / uniformly from S
- U_n x is chosen from the set of all n-bit strings
- $\mu(\cdot)$ means the negligible function can take any input. Negligible functions decrease faster than inverse polynomial as n increases
- must use positive polynomial, if not, maybe it won't be negligible. We want $\mu(n) < \frac{1}{p(n)}$
- λ is an empty string

$$X = \{X(a,n)\}_{a \in \{0,1\}^*; n \in \mathbb{N}}$$

"A probability ensemble" is a collection or family of random variables, denoted by $X = \{X(a,n)\}$ i.e. X represents the set of $\{X(a,n)\}$.

- Set $X = \{X(a,n)\}$ defines the set of random variables X
- Set Subscript $a \in \{0,1\}^*; n \in \mathbb{N}$ defines the indexing, that is, exactly what values of a, n can take for infinitely any element in set X. e.g. $X('01', 3)$ is the index of a random variable X where a is a binary string of any finite length "0, 1, 01, 000", n is a natural number 1,2
- $\{0,1\}^*$ is the Kleene star operation, means all finite strings, an infinite set because there's no limit to the length
- $n \in \mathbb{N}$ means n can be any natural number, also an infinite set
- indexing gives us an address or a way to talk about 1 specific random variable rather than the collection
- "probability ensemble" is a term in cryptography / probability theory referring to a collection or family of probability distributions or random variables. Used to describe systems where behaviours depend on on input length, security parameter, etc
- "ensemble" means we're dealing with a collection of probabilistic objects rather than a single fixed distribution

$$|\Pr[D(X(a,n)) = 1] - \Pr[D(Y(a,n)) = 1]| \leq \mu(n)$$

The (absolute difference) of the probability that the distinguisher D outputs 1 when given a sample from $X(a,n)$ and the probability D outputs 1 when given a sample from $Y(a,n)$ is $\leq$ the negl. function $\mu(\cdot)$

Notes:

- D is a PPT algorithm trying to distinguish between samples from X and Y, not guessing the bit
- $D's$ output is binary $\{0,1\}$. Output 1 means "The sample came from X" or "This is a real sample" i.e. distinguish
- We look at the difference in probability of D outputting 1 for X vs Y
- a negl. difference means D can't distinguish
- absolute value —— means we only want the magnitude of the difference, doesn't matter which is larger
- $\mu(n)$ being a negl. function means the difference becomes smaller as the security parameter grows larger