1 An import property of XOR

Y is a rand var over $\{0,1\}^n$, X is an independent uniform var over $\{0,1\}^n$ Then Z:=$X \oplus Y$ is uniform var over $\{0,1\}^n$

2 Symmetric ciphers: definition

A cipher defined over (K, M, C) is a pair of "efficient" algs (E,D) Where $E : K \times M \to C, D : K \times C \to M$ s.t. $\forall m \in M$ D(k, E(K,M)) == M

3 Information theoretic security

A cipher (E, D) over (K, M, C) has perfect secrecy if $\forall m_0, m_1 \in M, (|m_0| == |m_1|)$, and $\forall c \in C$ $Pr[E(k, m_0) == Pr[E(k, m_1)]]$ where k $\leftarrow rand$ K

4 PRG must be unpredictable

We say $G : K \to \{0,1\}^n$ is predictable if: $\exists$ efficient alg α and $\exists i, 1 \leq i \leq n-1$ s.t. $Pr[\alpha(G(k)|_{1,\ldots,i}) = G(k)|_{i+1}] \geq \frac{1}{2} + \epsilon$

5 Secure PRGs: crypto definition

Def we say that G:K $\to$ $\{0,1\}^n$ is a secure PRG if $\forall$ "eff" stat test A : $Adv_{PRG}[A, G]$ is "negligible"

6 PRF: pseudo random function

Def: let F: $K \times X \to Y$ be a PRF Funs[X,Y]: the set of all functions from X to Y $S_F = \{F(K, \bullet)\ s.t.\ k \in K\} \subseteq Funs[X, Y]$
Intuition: a PRF is secure if a random function in Funs[X,Y] is indistinguishable from a random function in S_F