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 Symmetic ciphers: defination

A cipher defined over (K, M, C) is a pair of "efficient" algs (E,D) Where $E : K \times M \rightarrow C, D : K \times C \rightarrow M$ 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