Cryptography

Vayasix

2015 11.7

Part I
Stream Ciphers

1 Information theoretic security and one time pad

1.1 Symmetric Ciphers

Def: a cipher defined over $\{\mathcal{K}, \mathcal{M}, \mathcal{C}\}$ is a pair of 'efficient' (usually efficient means running in polynomial time) algs E, D where

$$E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}, \quad D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

$$s.t. \forall m \in \mathcal{M}, k \in \mathcal{K} : \mathcal{D}(k, \mathcal{E}(k, m)) = m$$

NOTE: E is randomized, $\quad D$ is deterministic.

1.2 One Time Pad

feature: very fast enc/dec, but long keys as long as plaintext
$enc : m \oplus k = c,\ dec : c \oplus k = m$

1.3 Information Theoretic Security (Shannon 1949)

Shannon's definition, basic idea is
CT should reveal no 'information' about PT

Def: A cipher (E, D) over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ is perfectly secure if

$$\forall m_0, m_1 \in \mathcal{M},\ c \in \mathcal{C}$$

$$Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$$

where k is uniform in $\mathcal{K}$ ($k \overset{R}{\leftarrow} K$)