2021-04-01

Apr 1, 10:25 AM

IIC 3253

Perf. Secrecy:

$\forall m_1, m_2 \in M,\ c_0 \in C$

$$\Pr_{k \in K}[Enc(k, m_1) = c_0] = \Pr_{k \in K}[Enc(k, m_2) = c_0]$$

Teorema:

Si un sistema criptográfico tiene P.S. entonces $|K| \geq |M|$.

Dem: Por contr. sup. $|K| < |M|$

Sea $m_0 \in M$, $k_0 \in K$, $c_0 := Enc(k_0, m_0)$

$$S_0 = \{m \in M \mid \exists k \in K \text{ t.q. } Enc(k, m) = c_0\}$$

Cada mensaje en S_0 corresponde exactamente a 1 llave.

$$|S_0| \leq |K| < |M|$$

$\Rightarrow \exists m' \in M \setminus S_0$

$$\Pr_{k \in K}[Enc(k, m_0) = c_0] > 0$$

$$\Pr_{k \in K}[Enc(k, m') = c_0] = 0$$

$\Rightarrow \Leftarrow$

$$Dec(k, Enc(k, m)) = m$$

$m_1 \neq m_2$, $k \in K$

$$\Rightarrow \quad Enc(K, m_1) \neq Enc(K, m_2)$$

$$Dec(k, c_0) = ?$$