SEMANTIC SECURITY

STREAM CIPHERS 6

CIFRA SEGURA:

* Atacante obtém texto cifrado e: 1) não consegue recuperar a chave.
2) não consegue recuperar texto em claro.
3) Cifra não revela nada sobre o texto em claro.

* (E,D) tem segredo perfeito se:

$\forall m_0, m_1 \in \mathcal{M} \; (|m_0| = |m_1|)$

$\{E(K, m_0)\} = \{E(K, m_1)\}$ onde $K \xleftarrow{R} \mathcal{K}$

ou

$\forall m_0, m_1 \in \mathcal{M} \; (|m_0| = |m_1|)$

$\{E(K, m_0)\} \stackrel{s}{\equiv}_p \{E(K, m_1)\}$ onde $K \xleftarrow{R} \mathcal{K}$

→ definições ainda muito sólidas, adversário tem exposição de $m_0, m_1 \in \mathcal{M}$

SEGURANÇA SEMÂNTICA (chave de uso único)

* DEF: "E" é semanticamente seguro se para todo "eff." de A: $Adv_{SS}[A, E]$ for "neg".

⇒ Para todo $m_0, m_1 \in \mathcal{M}$: $\{E(K, m_0)\} \stackrel{s}{\equiv}_p \{E(K, m_1)\}$