12/04/2023

CRIPTOGRAFÍA

Tarea 1.

[P1] Perfectamente indistinguible

$$Pr[C=c \mid M=m_1] = Pr[C=c \mid M=m_2]$$

$$Pr[E_k(m_1)=c] = Pr[E_k(m_2)=c]$$

Confidencialidad perfecta

$$Pr[M=m \mid C=c] = Pr[M=m]$$

Perfectamente indistinguible $\leftrightarrow$ Confidencialidad perfecta

$PrivK_{A,SE}$ → un juego o esquema de cosas

a) Adversario A: entrega m_1 y m_2
b) $k \xleftarrow{R} Gen$ y $b \in \{0,1\}$ b=1bit → preguntar quien es m_b
c) $C \leftarrow Enc_k(m_b)$ y se envía C al adversario
d) A entrega $b' \in \{0,1\}$
e) Resultado final: 1 si $(PrivK_{A,SE}=1)$ $b=b'$
0 else

Suposición:
$Pr[PrivK_{A,SE}=1] = 1/2$ → irla transformando hasta que nos de la expr que queremos.

PDQ: SE es perfectamente indistinguible

Nota: demostración por construcción o por contradicción

[P2] 2-SDES: lo mismo que DES pero solo aplicando dos rondas de la red de Feistel.

PDQ: 2-SDES no es un PRF

Idea: Demostrar que la ventaja del adversario es cercana a 1 dado un número bajo de preguntas de un adversario

Pregunta: ¿En qué influyen las rondas de la red de Feistel?

[P3] Cifrador de bloque

$$E: \{0,1\}^{n \times n} \times \{0,1\}^n \rightarrow \{0,1\}^n$$

$E_K(M) = K \cdot M$ para $M \in \{0,1\}^n$, $K \in \{0,1\}^{n \times n}$

$(\cdot)$ es AND
$(+)$ es XOR

a) Ataque de recuperación de clave para el cifrador E
Utilizar
Seguridad PRF implica seguridad KR

b) Mejora de E:

$$E'_{K_1, K_2}(M) = K_1 \cdot M + K_2$$

con $K_1 \in \{0,1\}^{n \times n}$ y $K_2 \in \{0,1\}^n$
PDQ: E' no es un PRF seguro
Idea: Ataque de adversario A con $Adv \approx 1$ (utilizando cantidad de preguntas.)
(a) Hay que encontrar la clave K (un ataque)
Se puede diseñar un ataque.