Pregunta 2

Esquema criptográfico sobre los espacios $\mathcal{M} = K = C = \{0,1\}^n$

Gen NO permite claves cuyo primer bit sea 0 el resto es con distribución uniforme

¿PRP? Una vuelta

Primero hay que recordar el juego que usamos para definir una PRP

1.- Verificador elige $b \in \{0,1\}$ con dist. uniforme

1.1.- Si $b = 0$, entonces elige una clave $k \in K$ según Gen y define $f(x) = Enc(k, x)$

1.2.- Si $b = 1$, entonces elige una permutación π con dist. uniforme y define $f(x) = \pi(x)$

2.- El adversario elige una palabra $y \in \{0,1\}^n$, el verificador responde con $f(y)$

3.- El adversario indica si $b = 0$ o $b = 1$, y gana si su elección es correcta.

Lo único que sabemos del juego es que las llaves de la forma $0x$ con $x \in \{0,1\}^{n-1}$ no están permitidas, por lo tanto

$$|K| < |M| < |C|$$

Además, con esto sabemos que la cantidad de posibles llaves es 2^{n-1}

Como vimos en clases la probabilidad de ganar el juego es

$$Pr(gana) = Pr(gana \mid b=0) \cdot Pr(b=0) + Pr(gana \mid b=1) \cdot Pr(b=1) =$$

$$\frac{1}{2} Pr(gana \mid b=0) + \frac{1}{2} Pr(gana \mid b=1)$$

En el caso en que $\boxed{b=0}$ se use $f(x) = Enc(k, x)$

Asumo que el adversario es capaz de elegir un mensaje tal que el 0 al inicio de la llave le de un indicio de que lo que ocurre es que se encripte

entonces

$$Pr(gana \mid b=0) = 1$$

Tal como vimos en clases

$$Pr(\text{gana} \mid b = 1) = Pr(\pi(y) \neq Enc(k, y))$$

$$= 1 - Pr(\pi(y) = Enc(k, y))$$

En clases vimos la probabilidad para una llave en particular, pero en este caso tenemos 2^{n-1} llaves a considerar

Ya visto en clases → con un k particular la probabilidad es $\frac{1}{2^n}$

Como $P(A \circ B) = P(A) + P(B)$

$$Pr(\pi(y) = Enc(k, y)) = \sum_{1}^{2^{n-1}} \frac{1}{2^n} = \frac{1}{2}$$

Entonces

$$Pr(\text{gana}) = \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

Entonces queda demostrado lo pedido.