Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
Criptografía y Seguridad Computacional

Pregunta 2

28 de abril de 2022

Pablo Brancoli - 18642578

Primero que nada como Gen no admite claves cuyo primer bit sea 0, podemos asumir que el largo de Gen va a ser $n/2$, y por el enunciado entonces, Gen elige claves con distribución uniforme sobre $n/2$.

Dado que $3/4$ es significativamente mayor a $1/2$, tenemos que demostrar que la probabilidad de que el adversario gane en la ronda 1 es $3/4$. Vamos a tener que:

$$Pr(AdversarioGane) = Pr(AdversarioGane|b = 0) * 1/2 + Pr(AdversarioGane|b = 1) * 1/2$$

Pensemoslo asi: El espacio de los textos Encriptados va a ser $2^{n-1}!$, dado que van a ser encriptados por todas las claves cuyo primer bit sea 1, asumimos asi que el adversario tiene poder computacional infinito y sabe cuales textos son posibles encriptados. Decimos así que si el verificador le entrega un texto perteneciente a los posibles encriptados el adversario responde con $b = 0$, por otro lado si el verificador le entrega un texto que no pertence a los encriptados, el adversario responde con $b = 1$. Asi tenemos que:

$$Pr(AdversarioGane|b = 0) = 1$$

Dado que se eligió $b = 0$ el adversario si o si va a responder con $b = 0$ ya que el texto pertenecería a los posibles encriptados.

Por otro lado la Pr(Adversario Gane $|b = 1)$ va a ser la probabilidad de que la permutación no sea igual a la encriptación, es decir $\Pr(\pi(y) \neq Enc(k, y))$,ya que si esto pasa el adversario responderia erroneamente con $b = 0$, pero si el texto no pertenece a los posibles encriptados responderia con $b = 1$

$Pr(\pi(y) \neq Enc(k, y))$ = Casos Favorables / Casos Totales

Como vimos en clases el numero total de permutaciones es $2^n!$, por que esos serán nuestros casos totales.

En cuanto a los casos favorables, tenemos que estos van a ser todos los casos donde la encriptacion no sea igual a la permutacion. Ahora bien sabemos que la encriptacion es una funcion 1-1 y que el espacio de las llaves es todos los cuales el primer bit es 1 es decir $2^{n-1}!$. Por lo que podemos asumir que el espacio de las llaves y la encriptacion es el mismo. Es decir $1 - 2^{n-1}!$ mensajes pertenecen a pseudo random.

$$|Enc(k, y)| = |Gen(k)|$$
$$Pr(\pi(y) \neq Enc(k, y)) = 1 - Pr(\pi(y) = Enc(k, y))$$
$$Pr(\pi(y) \neq Enc(k, y)) = 1 - 2^{n-1}!/2^n!$$
$$= 1 - 2^{n-1}!/(2^{n-1}! * 2)$$
$$= 1 - 1/2$$
$$= 1/2$$

Entonces:

$$Pr(AdversarioGane) = Pr(AdversarioGane|b = 0) * 1/2 + Pr(AdversarioGane|b = 1) * 1/2$$

$$Pr(AdversarioGane) = 1 * 1/2 + 1/2 * 1/2$$
$$Pr(AdversarioGane) = 3/4$$

Lo cual por el enunciado sabemos que es una probabilidad significativamente mayor a $3/4$, es decir este esquema no es una pseudo-random permutation de una ronda.