Tarea 1 criptografía

José Lara Hinojosa

Mayo 2021

Pregunta 4

El problema se puede modelar como:

$$P(AdversarioGane) = P(AdversarioGane|b = 0) \cdot p(b = 0) + P(AdversarioGane|b = 1) \cdot p(b = 1)$$

Primero tenemos que separar los dos casos principales del problema, que divide según el valor de b:
b=0:
Para esta pregunta ocuparemos la propiedad de los xor, primero tomaremos los 40 mensajes $m_1, ..., m_{40}$ y sus 40 encriptaciones correspondientes $c_1, ..., c_{40}$ desde el verificador con cada mensaje distinto del anterior.
La propiedad de la que hablamos consiste en que si dos mensajes estan encriptados con una misma llave sucede lo siguiente:

$$(\forall m_1, m_2 \in M, k \in K) m_1 \oplus m_2 = Enc(k, m_1) \oplus Enc(k, m_2) \tag{1}$$

Esto debido a que las llaves se cancelan por propiedad conmutativa del xor.
Como tenemos los mensajes podemos hacer el xor entre ellos con distintas combinaciones y verificar que alguna de las encriptaciones xorteadas den lo mismo, con lo cual sabríamos que muy probablemente es OTP apostando por b = 0.
Sabiendo esto nuestro problema se reduce a que se repita al menos una llave en todo el set de llaves K' en alguna de los 40 mensajes que encripto el verificador, la cual fue elegida con probabilidad uniforme.
Este problema es análogo al problema del cumpleaños visto en clases, el cual nos dice que (sacado de wikipedia):

$$1 - p = \begin{cases} 1 - \frac{365!}{365^n (365-n)!}, & 1 \leq n \leq 365 \\ 1, & n > 365 \end{cases} \tag{2}$$

Lo que nos dice que teniendo n personas la probabilidad de que dos tengan cumpleaños en el mismo dia es $1 - \frac{365!}{365^n (365-n)!}$
En nuestro caso queremos calcular la probabilidad de que exista una colision (en este caso

que se encripte con la misma llave) con 40 posibles llaves sacadas de manera uniforme desde un conjunto de 1000 llaves (K'), por lo que la probabilidad sería:

$$P(AdversarioGane|b=0) = 1 - \frac{1000!}{1000^{40} \cdot (1000-40)!} \tag{3}$$

$$= 0{,}4536 \tag{4}$$

b=1:
Para este caso tenemos que ver la probabilidad de que el adversario pierda, es decir, en los 40 mensajes y 40 encriptaciones que tenemos, algún par de mensajes nos da

$$m_1 \oplus m_2 = \pi(m_1) \oplus \pi(m_2) \tag{5}$$

Lo que nos haría creer que estamos frente a OTP cuando en verdad no lo estamos.
Para 2 rondas como lo visto en clases si lo pensamos como una tabla de 2^n entradas teniendo un mensaje fijado que sería $m_1 -> \pi(m_1)$ tendremos $2^n - 1$ entradas libres, luego habrá que fijar otro mensaje m_2 el cual justo será el que nos cumple la propiedad

$$P(\text{perder en ronda 2}) = \frac{(2^n - 1 - 1)!}{(2^n - 1)!} \tag{6}$$

Luego para 3 rondas tendremos fijados m_1 y m_2, que sabemos que entre ellos no cumplen la propiedad, por lo tanto tenemos 2 posibles valores que harian cumplir la propiedad, luego tendríamos

$$P(\text{perder en ronda 3} \mid \text{no perdi en ronda 2}) = \frac{2 \cdot (2^n - 2 - 1)!}{(2^n - 2)!} \tag{7}$$

Luego para 4 rondas tendremos fijados m_1, m_2 y m_3, que sabemos que entre ellos no cumplen la propiedad, por lo tanto tenemos 3 posibles valores que harian cumplir la propiedad, luego tendríamos

$$P(\text{perder en ronda 4} \mid \text{no perdi en ronda 3}) = \frac{3 \cdot (2^n - 3 - 1)!}{(2^n - 3)!} \tag{8}$$

Finalmente para k rondas tendremos

$$\frac{k \cdot (2^n - (k-1) - 1)!}{(2^n - (k-1))!} \tag{9}$$

Reemplazando k con el numero de rondas que es 40

$$P(\text{perder en ronda 40} \mid \text{no perdi en ronda 39}) = \frac{39 \cdot (2^{128} - 38))!}{(2^{128} - (39))!} \tag{10}$$

$$= \frac{39}{2^{128} - 39} = 0{,}00000.... \tag{11}$$

Finalmente la probabilidad total de perder en alguna de las rondas es la suma de las probabilidades de los casos anteriores.
En este punto ya es claro ver que la probabilidad de que pierda en la ronda 2 es insignificante ya que tiende a 0 ya que 2^{128} es muy grande y al ser el denominador más grande que el númerador quedará un 2^{128} abajo el cual es un numero demasiado grande.
A medida que fijamos mensajes notamos que la probabilidad aumenta ya que el numerador aumenta mientras que el denominador se achica, sin embargo esto es insignificante a lo que aporta en el denominador el 2^{128}.
Finalmente la probabilidad de perder en las 40 rondas sigue siendo cercana a 0 luego de sumarlas.
Por lo tanto tendremos que la probabilidad de ganar sería:

$$P(AdversarioGane|b = 1) = 1 - 0{,}00000000.... \tag{12}$$
$$= 1 \tag{13}$$

Resultado final:
Como sabemos que tirar una moneda es una probabilidad de 1/2 tendremos que el resultado final será

$$P(AdversarioGane) = \frac{1}{2} \cdot 0{,}4536 + \frac{1}{2} \cdot 1 = 0{,}7268 \tag{14}$$

Lo cual es muy cercano a lo que habíamos a 3/4.