Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencia de la Computación

IIC3253 — Criptografía y Seguridad Computacional

Sebasthian von Bergen (15635635)

Tarea 1 – Respuesta Pregunta 2

Sea un esquema criptográfico (GEN, ENC, DEC) definido sobre los espacions $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Además, la funcion generadora de clave siempre define el primer bit de las claves $k \in \mathcal{K}$, $k_0 = 0$.

Sea b=0, el caso donde el verificador esta utilizando el algoritmo ENC, con una clave generada k. El adversario le entrega un mensaje m al verificador y recibe de vuelta $c_0 = \text{ENC}(m,\ k)$. Sea b=1, el caso donde el verificador esta utilizando una permutación aleatoria π. El adversario le entrega m al verificador y recibe $c_0 = \pi(m)$.

Dado que el adversario no conoce en que mundo esta (b=0 o b=1) tendra que adivinar. El adversario puede crear una tabla que contenga todas las codificaciones de ENC(m, k), para las 2^{n-1} llaves posibles. Esto se puede hacer porque sabemos que el primer digito es siempre 0. El tamaño de esta tabla es 2^{n-1}.

Luego comparamos el mensaje que recibimos c_0 del verificador con las entradas de la tabla. Si coincide con alguna de las entradas entonces decidimos que el verificador esta utilizando el esquema criptográfico (b=0). Si no esta presente entonces sabemos con 100% de certeza que se esta utilizando una permutación ya que es imposible obtener ese c_0 utilizando las llaves posibles y el esquema criptográfico.

El único caso en donde nos equivocamos es cuando recibimos de la permutacion uno de los textos cifrados posibles por coincidencia. Para analisar la probabilidad podemos comparar el tamaño de las tablas, la que creamos nosotros y la tabla de permutacion. Sabemos que el tamaño de la permutacion es 2^n y que no hay colisiones. En cambio la tabla generada con el esquema tiene un tamaño de 2^{n-1}, la mitad del tamaños. La probabilidad de elegir una entrada en la tabla π que este presente en la tabla que creamos con el esquema es $\frac{2^{n-1}}{2^n} = \frac{1}{2}$.

Podemos calcular nuestra probabilidad de exito final:

$$\begin{gathered}
\Pr[\text{adivinar } b=0 | b=0] \cdot \Pr[b=0] + \Pr[\text{adivinar } b=1 | b=1] \cdot \Pr[b=1] \\
\Pr[\text{adivinar } b=0 | b=0] = 1 \\
\Pr[\text{adivinar } b=1 | b=1] = \frac{1}{2} \\
\Pr[b=0] = \Pr[b=1] = \frac{1}{2} \\
1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}
\end{gathered}$$

Por lo tanto, dada una ronda, el adversario puede adivinar correctamente si el verificador esta utilizando el esquema con una probabilidad significativamente mayor a $\frac{1}{2}$. El adversario tiene que hacer $O(O(ENC) \cdot n)$ operaciones, lo que es polinomial y por lo tanto una cantidad aceptable.