Recuerde que ...

Definición de una noción de seguridad debe incluir:

- Un modelo de amenaza, que define las capacidades de un **adversario**
- Una garantía de seguridad, lo cual normalmente se traduce en definir qué significa que el adversario no tenga éxito en su **ataque**

Vamos a definir una primera noción de seguridad

Nos va a permitir mostrar que OTP no es seguro si la clave es reutilizada

- Va a formalizar la intuición de las clases anteriores

El escenario

Consideramos un largo n fijo:

- Llaves: $\mathcal{K} = \{0,1\}^n$
- Mensajes: $\mathcal{M} = \{0,1\}^n$
- Textos cifrados: $\mathcal{C} = \{0,1\}^n$

Esquema criptográfico: (Gen, Enc, Dec)

Juego para definir una pseudo-random permutation

1. **Verificador** elige $b \in \{0, 1\}$ con distribución uniforme (tira una moneda)
    1.1. Si $b = 0$, entonces elige una clave $k \in \mathcal{K}$ según la distribución Gen y define $f(x) = Enc(k, x)$
    1.2. Si $b = 1$, entonces elige una permutación π con distribución uniforme y define $f(x) = \pi(x)$

Juego para definir una pseudo-random permutation

2. El **adversario** elige una palabra $y \in \{0,1\}^n$, el verificador responde con $f(y)$
3. El paso 2. es repetido q veces
4. El adversario indica si $b = 0$ o $b = 1$, y gana si su elección es correcta

¿Cuál es la probabilidad de que el adversario gane?

- Esto depende de la cantidad de rondas q
- Si el adversario tira una moneda en el paso 4., entonces su probabilidad de ganar es 1/2

Pseudo-random permutation (PRP)

Decimos que (Gen, Enc, Dec) es una pseudo-random permutation si no existe un adversario que pueda ganar el juego con una probabilidad significativamente mayor a 1/2

¿Cuáles son las capacidades del adversario?

No imponemos restricciones en las capacidades computacionales del adversario

Podríamos tener una noción más débil donde el adversario puede realizar una cantidad de operaciones que es polinomial en n

- Por ejemplo, solo puede realizar n^2 operaciones

¿Qué restricciones imponemos sobre el ataque?

Debemos definir qué significa que la probabilidad de ganar el juego sea significativamente mayor a 1/2

- Por ejemplo, esta probabilidad podría ser 3/4

También tenemos que indicar cuál es el número de rondas q

Un primer ejemplo

Considere un esquema criptográfico (Gen, Enc, Dec) tal que:

- $Gen(k_0) = 1$ para una clave fija $k_0 \in \mathcal{K}$
- $Gen(k) = 0$ para todo $k \in \mathcal{K}$ tal que $k \neq k_0$

Vamos a demostrar que este esquema criptográfico no es una PRP con una ronda ($q = 1$)

¿Cómo puede ganar el juego el adversario?

La siguiente es su estrategia en el juego:

- En el paso 2. toma $y = 0^n$ y recibe $f(y)$ como respuesta del verificador
- Si $f(y) = Enc(k_0, y)$ entonces indica que b es igual a 0, sino indica que b es igual a 1

¿Puede el adversario equivocarse al indicar el valor de b? ¿Cuál el la probabilidad de que gane el juego?

La probabilidad de ganar el juego

$$\Pr(\text{Adversario gane el juego}) =$$

$$\Pr(\text{Adversario gane el juego} \mid b = 0) \cdot \Pr(b = 0) +$$
$$\Pr(\text{Adversario gane el juego} \mid b = 1) \cdot \Pr(b = 1) =$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) +$$
$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1)$$

La probabilidad de ganar el juego

$$\Pr(\text{Adversario gane el juego} \mid b = 0) = 1$$

$$\Pr(\text{Adversario gane el juego} \mid b = 1) = \Pr_{\pi}(\pi(y) \neq Enc(k_0, y))$$

En este caso el verificador elige una permutación $\pi : \{0,1\}^n \to \{0,1\}^n$ con distribución uniforme

- Si $\pi(y) = Enc(k_0, y)$, entonces el adversario da la respuesta equivocada

Calculando $\Pr(\pi(y) \neq Enc(k_0, y))$

$$\Pr(\pi(y) \neq Enc(k_0, y)) = 1 - \Pr(\pi(y) = Enc(k_0, y))$$

$$\Pr(\pi(y) = Enc(k_0, y)) = \frac{\text{casos favorables}}{\text{casos totales}}$$

Casos totales: número de permutaciones $\pi : \{0,1\}^n \to \{0,1\}^n$

- Este número es igual a $(2^n)!$

Calculando $\Pr(\pi(y) \neq Enc(k_0, y))$

$$\Pr(\pi(y) = Enc(k_0, y)) = \frac{\text{casos favorables}}{(2^n)!}$$

Casos favorables: número de permutaciones $\pi : \{0,1\}^n \to \{0,1\}^n$ tales que $\pi(0^n)$ es igual al valor fijo $Enc(k_0, 0^n)$

- Este número es igual a $(2^n - 1)!$

Calculando $\Pr(\pi(y) \neq Enc(k_0, y))$

$$\Pr(\pi(y) = Enc(k_0, y)) = \frac{(2^n - 1)!}{(2^n)!} = \frac{1}{2^n}$$

$$\Pr(\pi(y) \neq Enc(k_0, y)) = 1 - \frac{1}{2^n}$$

El cálculo final

$$\Pr(\text{Adversario gane el juego}) =$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) +$$
$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1) =$$

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot (1 - \frac{1}{2^n}) = 1 - \frac{1}{2^{n+1}}$$

El adversario gana el juego con una probabilidad significativamente mayor a 1/2

- Para convencerse de esto considere $n = 10$ y $n = 100$

Consideremos ahora OTP

Dado que $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$, debemos realizar las operaciones de OTP en módulo 2

$$
\begin{array}{rll}
 & 0\,1\,1\,0\,1\,0\,0\,0\,1\,1 & \longleftarrow\ m \\
+ & 1\,0\,0\,1\,1\,0\,1\,1\,0\,1 & \longleftarrow\ k \\
\hline
\bmod 2 & 1\,1\,1\,1\,2\,0\,1\,1\,1\,2 & \\
\hline
 & 1\,1\,1\,1\,0\,0\,1\,1\,1\,0 & \longleftarrow\ c
\end{array}
$$

OTP no es una PRP con dos rondas

La estrategia del adversario:

- En el paso 2. toma $y_1 = 0^n$ e $y_2 = 1^n$, y recibe $f(y_1)$ y $f(y_2)$ como respuesta del verificador
- Si $y_2 + f(y_1) = f(y_2)$ entonces indica que b es igual a 0, sino indica que b es igual a 1

¿Cuál es la idea detrás de esta estrategia?

Si $b = 0$, el verificador está usando OTP y existe una clave k tal que:

$$y_1 + k = f(y_1)$$
$$y_2 + k = f(y_2)$$

Como $y_1 = 0^n$, se tiene que $k = f(y_1)$, y se concluye que $y_2 + f(y_1) = f(y_2)$

La probabilidad de ganar el juego de dos rondas

$$\Pr(\text{Adversario gane el juego}) =$$

$$\Pr(\text{Adversario gane el juego} \mid b = 0) \cdot \Pr(b = 0) +$$
$$\Pr(\text{Adversario gane el juego} \mid b = 1) \cdot \Pr(b = 1) =$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) +$$
$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1)$$

La probabilidad de ganar el juego de dos rondas

$$\Pr(\text{Adversario gane el juego} \mid b = 0) = 1$$

$$\Pr(\text{Adversario gane el juego} \mid b = 1) = \Pr_{\pi}(\pi(y_2) \neq y_2 + \pi(y_1))$$

En este caso el verificador elige una permutación $\pi : \{0,1\}^n \to \{0,1\}^n$ con distribución uniforme

- Si $\pi(y_2) = y_2 + \pi(y_1)$, entonces el adversario da la respuesta equivocada

Calculando $\Pr(\pi(y_2) \neq y_2 + \pi(y_1))$

$$\Pr(\pi(y_2) \neq y_2 + \pi(y_1)) = 1 - \Pr(\pi(y_2) = y_2 + \pi(y_1))$$

$$\Pr(\pi(y_2) = y_2 + \pi(y_1)) = \frac{\text{casos favorables}}{\text{casos totales}}$$

Casos totales: número de permutaciones $\pi : \{0,1\}^n \to \{0,1\}^n$

- Este número es igual a $(2^n)!$

Calculando $\Pr(\pi(y_2) \neq y_2 + \pi(y_1))$

$$\Pr(\pi(y_2) = y_2 + \pi(y_1)) = \frac{\text{casos favorables}}{(2^n)!}$$

Casos favorables: número de permutaciones $\pi : \{0,1\}^n \to \{0,1\}^n$ tales que $\pi(1^n) = 1^n + \pi(0^n)$

- Este número es igual a $2^n \cdot (2^n - 2)!$

Calculando $\Pr(\pi(y_2) \neq y_2 + \pi(y_1))$

$$\Pr(\pi(y_2) = y_2 + \pi(y_1)) = \frac{2^n \cdot (2^n - 2)!}{(2^n)!} = \frac{1}{2^n - 1}$$

$$\Pr(\pi(y_2) \neq y_2 + \pi(y_1)) = 1 - \frac{1}{2^n - 1}$$

El adversario gana el juego con una probabilidad significativamente mayor a 1/2

$$\Pr(\text{Adversario gane el juego}) =$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) +$$

$$\frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1) =$$

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot (1 - \frac{1}{2^n - 1}) = 1 - \frac{1}{2 \cdot (2^n - 1)}$$