DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
ESCUELA DE INGENIERÍA
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

IIC3253 - Criptografía y Seguridad Computacional (I/2023)

Ayudantía 2

Ayudantes: Susana Figueroa (sfigueroa3@uc.cl) Chris Klempau (christian.klempau@uc.cl)

Pregunta 1: OTP

(a) Correctitud de OTP

Demuestre que: $\forall_{k \in \mathcal{K}} \quad Dec_k(Enc_k(m)) = m$

Solución:

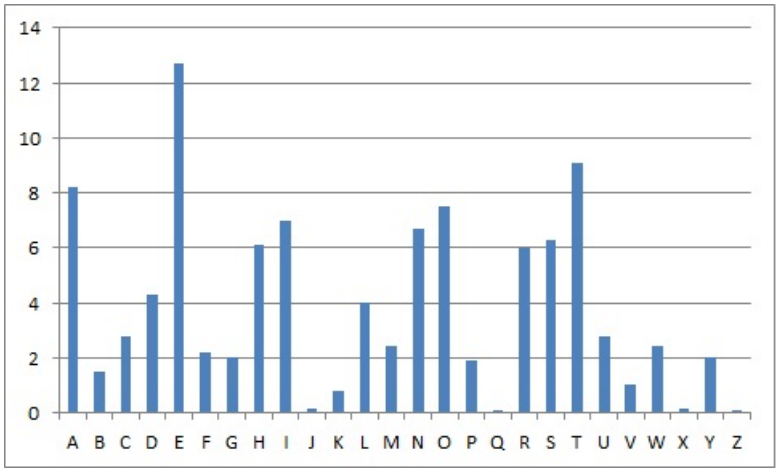
$$Enc_k(m) = (m + k) \mod N$$
$$Dec_k(c) = (c - k) \mod N$$
$$\rightarrow Dec_k(Enc_k(m)) = (m + k) \mod N - k) \mod N$$
$$\Leftrightarrow (m + k) - k) \mod N$$
$$\Leftrightarrow (m) \mod N$$
$$\Leftrightarrow m$$

(b) Modelos de ataque para OTP (al reutilizar llaves)

¿Bajo qué modelos de ataque es seguro OTP?
1. Texto cifrado
2. Texto plano
3. Texto plano elegido
4. Texto cifrado elegido

Solución:

1. Texto cifrado NO es seguro, bajo análisis de frecuencia.



2. Texto plano
Tenemos $(m_0, c_0), (m_1, c_1), ...$

Sabemos que $m_0 \oplus k = c_0$.
Lo anterior es equivalente a $k \oplus m_0 = c_0$.
Luego, operamos por $(\oplus m_0)$ a ambos lados.

$$(k \oplus m_0) \oplus m_0 = c_0 \oplus m_0$$
$$k \oplus (m_0 \oplus m_0) = c_0 \oplus m_0$$
$$k \oplus (0^N) = c_0 \oplus m_0$$
$$k = c_0 \oplus m_0$$

Ahora que tenemos k, podemos descifrar c_i no visto, sin necesidad de saber el mensaje de antemano.

3. y 4. son análogos, ya que basta tener un par m, c para deducir k.

Pregunta 2: Perfect Secrecy

Demuestre las definiciones alternativas de *perfect secrecy*:

(a) **Definición alternativa 1:**

"La probabilidad de ver cualquier texto cifrado sin conocimiento previo es la misma que la probabilidad de ver dicho texto cifrado conociendo el mensaje de antemano."

Solución:

Sea $\mathbb{D}$ una distribución sobre $\mathcal{M}$ y $\mathbb{F}$ una distribución sobre $\mathcal{C}$.
Se quiere demostrar que:

$$\Pr_{\substack{c\sim\mathbb{F}\\k\sim Gen}}\left[c = c_0 | Enc_k(m_0) = c\right] = \Pr_{c\sim\mathbb{F}}\left[c = c_0\right]$$

Reemplazamos c por $Enc_k(m)$.

$$\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0 | Enc_k(m_0) = Enc_k(m)\right] = \Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0\right]$$

Notamos el término $Enc_k(m_0) = Enc_k(m)$. Podemos decriptar por ambos lados:

$$Enc_k(m_0) = Enc_k(m)$$
$$Dec_k(Enc_k(m_0)) = Dec_k(Enc_k(m))$$

$$m_0 = m$$

Ahora reemplazamos en la ecuación anterior.

$$\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0 \mid m = m_0\right] = \Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0\right]$$

Ahora por el teorema de Bayes:

$$\frac{\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0 \ \cap \ m = m_0\right]}{\Pr_{m\sim\mathbb{D}}\left[m = m_0\right]} = \Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0\right]$$

Podemos reordenar

$$\frac{\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0 \ \cap \ m = m_0\right]}{\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[Enc_k(m) = c_0\right]} = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]$$

Notamos que si aplicamos Bayes de nuevo...

$$\Pr_{\substack{m\sim\mathbb{D}\\k\sim Gen}}\left[m = m_0 \ \mid \ Enc_k(m) = c_0\right] = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]$$

Obtenemos la definición de *perfect secrecy*!!

Falta demostrar la otra implicancia, esto queda propuesto para el lector :)

(b) **Definición alternativa 2:**

"La distribución de probabilidad sobre los mensajes es independiente de la distribución de probabilidad sobre los textos cifrados."

Solución:

Sea $\mathbb{D}$ una distribución sobre $\mathcal{M}$ y $\mathbb{F}$ una distribución sobre $\mathcal{C}$.
Si las distribuciones sobre los mensajes son independientes a la de los textos cifrados, significa que:

$$\Pr_{\substack{m\sim\mathbb{D}\\ c\sim\mathbb{F}}}\left[m = m_0 \wedge c = c_0\right] = \mathbb{D}(m_0)\cdot\mathbb{F}(c_0)$$

$$\Pr_{\substack{m\sim\mathbb{D}\\ c\sim\mathbb{F}}}\left[m = m_0 \wedge c = c_0\right] = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]\cdot\Pr_{c\sim\mathbb{F}}\left[c = c_0\right]$$

Cómo podemos interpretar $\Pr_{c\sim\mathbb{F}}\left[c = c_0\right]$? Es la probabilidad de que dado un mensaje m y una llave k, al encriptarlo se obtenga c_0.
Entonces si reemplazamos con esto queda,

$$\Pr_{\substack{m\sim\mathbb{D}\\ k\sim Gen}}\left[m = m_0 \wedge Enc_k(m) = c_0\right] = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]\cdot\Pr_{\substack{m\sim\mathbb{D}\\ k\sim Gen}}\left[Enc_k(m) = c_0\right]$$

Ahora reordenamos,

$$\frac{\Pr_{\substack{m\sim\mathbb{D}\\ k\sim Gen}}\left[m = m_0 \wedge Enc_k(m) = c_0\right]}{\Pr_{\substack{m\sim\mathbb{D}\\ k\sim Gen}}\left[Enc_k(m) = c_0\right]} = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]$$

Nos podemos dar cuenta de que el lado izquierdo de la ecuación equivale a la probabilidad condicionada (teorema de Bayes) de elegir un mensaje m_0 dado que $Enc_k(m) = c_0$.

$$\Pr_{\substack{m\sim\mathbb{D}\\ k\sim Gen}}\left[m = m_0 \mid Enc_k(m) = c_0\right] = \Pr_{m\sim\mathbb{D}}\left[m = m_0\right]$$

Esta es la definición original de *perfect secrecy*, aunque tenemos el mensaje cifrado no obtenemos información sobre el mensaje original.

Falta demostrar la otra implicancia, esto queda propuesto para el lector :)

Pregunta 3: PRP

[2022 - Tarea 1] Considere un esquema criptográfico (Gen, Enc, Dec) definido sobre los espacios $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$. Suponga además que Gen no permite claves cuyo primer bit sea 0, y que el resto de las claves son elegidas con distribución uniforme. Demuestre que este esquema no es una pseudo-random permutation con una ronda, si $\frac{3}{4}$ es considerada como una probabilidad significativamente mayor a $\frac{1}{2}$.

Solución:

A primera vista notamos que si PRP elige $b = 0$, es decir, encriptar con una llave generada por la función Gen, el espacio de llaves que entrega esta función es la mitad de las llaves posibles $\mathcal{K}$, debido a que la llave siempre empieza con 1, por lo que el adversario puede ganar mucha información con esto.

consideramos un adversario que ejecuta los siguientes pasos:

- El adversario entrega $y = 0^n$ al verificador y recibe como respuesta $f(y)$.
- Si $f(y) = Enc(k, y)$ para algún $k \in \{0,1\}^n$ tal que el primer bit de k es 1, entonces el adversario indica que $b = 0$, sino indica que $b = 1$.

Nótese que para implementar el segundo paso se deben considerar 2^{n-1} claves k en el peor de los casos. Vale decir, el adversario es un algoritmo de tiempo exponencial, lo cual no es un problema puesto que la definición de PRP no impone restricciones sobre su tiempo de funcionamiento.

Necesitamos calcular la probabilidad de que el adversario gane el juego, lo cual está dado por la siguiente expresión:

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

Si $b = 0$, entonces el verificador debe haber encriptado el mensaje $y = 0^n$ con una clave $k \in \{0,1\}^n$ tal que el primer bit de k es 1. Tenemos entonces que el adversario elige $b = 0$ y gana el juego. Se concluye que $\Pr(\text{Adversario gane el juego} \mid b = 0) = 1$. Si $b = 1$, entonces el verificador escoge al azar una permutación $\pi : \{0,1\}^n \to \{0,1\}^n$ y responde en el juego con el valor $f(y) = \pi(y)$. En este caso, tenemos que el adversario pierde el juego si $f(y) = Enc(k, y)$

para algún $k \in \{0,1\}^n$ tal que el primer bit de k es 1. Vale decir,

$$\begin{aligned}\Pr(\text{Adversario pierda el juego} \mid b = 1) &= \Pr_{\pi}\left(\bigvee_{\substack{k \in \{0,1\}^n : \\ \text{el primer bit de } k \text{ es } 1}} \pi(y) = Enc(k, y) \right) \\ &\leq \frac{2^{n-1} \cdot (2^n - 1)!}{(2^n)!} = \frac{1}{2}.\end{aligned}$$

Tenemos entonces que $\Pr(\text{Adversario gane el juego} \mid b = 1) \geq \frac{1}{2}$, de lo cual se concluye que:

$$\begin{aligned}&\Pr(\text{Adversario gane el juego}) = \\ &\quad \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 0) + \frac{1}{2} \cdot \Pr(\text{Adversario gane el juego} \mid b = 1) \geq \\ &\quad \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4},\end{aligned}$$

que era lo que queríamos demostrar.