

Clase 2: cifrado simétrico, secreto perfecto

Fernando Virdia, versión: 0.1, mayo 2025

2 One-Time Pads y secreto perfecto

Introducimos la noción de cifrado simétrico.

Definición 3 (SKES, cifrado simétrico). Sean $\mathcal{K}$, $\mathcal{M}$, $\mathcal{C}$ tres conjuntos. Decimos que $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ forman un cifrado simétrico (SKES, “secret-key encryption scheme”) con espacio de llaves $\mathcal{K}$, espacio de mensajes $\mathcal{M}$, y espacio de cifrados $\mathcal{C}$, si

- Gen es un algoritmo aleatorio, $\text{Gen}: \emptyset \rightarrow \mathcal{K}$;
- Enc es un algoritmo (posiblemente aleatorio), $\text{Enc}: \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{C}$;
- Dec es un algoritmo determinista $\text{Dec}: \mathcal{C} \rightarrow \mathcal{M}$;

tales que

$$\Pr_{\substack{k \sim \text{Gen}(), \\ \$ \text{ en Enc}}} [\text{Dec}(k, \text{Enc}(k, m; \$)) = m] = 1,$$

donde Gen, Enc y Dec son “eficientes”.

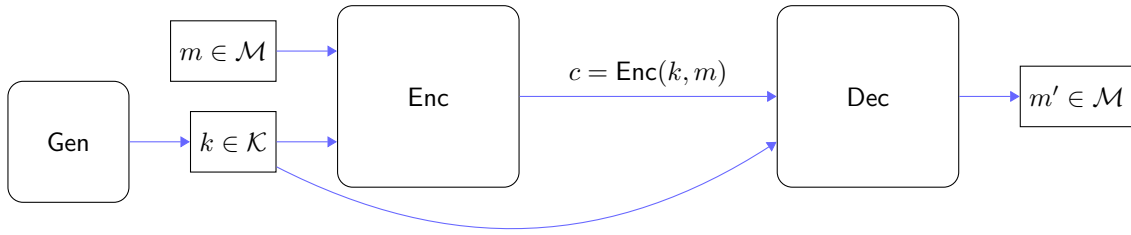


Figure 2: Uso de un cifrado simétrico. Consideramos el cifrado c ser expuesto al adversario.

Comentario 4. Generalmente consideramos $\mathcal{K}, \mathcal{M}, \mathcal{C} \subset \{0, 1\}^*$ en la criptografía simétrica.

Comentario 5. Generalmente consideramos $\mathcal{K}$ finito, y $\text{Gen}()$ consiste en muestrear la distribución uniforme $k \xleftarrow{\$} U(\mathcal{K})$.

Dada la sintaxis de un SKES, queremos encontrar definiciones que capturen la “seguridad” del mensaje cifrado $c = \text{Enc}(k, m)$.

PREGUNTA: Alguna idea de como definir la seguridad de c ?

1. Podríamos pedir que dado c , un adversario no aprenda k . Y si aprende m ?
2. Podríamos pedir que dado c , un adversario no aprenda m . Y si aprende la primera mitad de m ?
3. Podríamos pedir que dado c , no aprenda ninguna información sobre m . Y si alguna información es publica, por ejemplo que todo $m \in \mathcal{M}$ está escrito en castellano?

Definición 4 (Secreto perfecto, Shannon). Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un SKES. Decimos que Π ofrece secreto perfecto si dada la variable aleatoria $k \sim \text{Gen}()$,

$$\forall m_0, m_1 \in \mathcal{M}, c \in \mathcal{C}, \quad \Pr_{k \sim \text{Gen}()} [\text{Enc}(k, m_0) = c] = \Pr[\text{Enc}(k, m_1) = c].$$

Comentario 6. Un SKES que otorga secreto perfecto leakea que $m \in \mathcal{M}$. Por ejemplo, si $\mathcal{M} = \{0, 1\}^\ell$, leakea que $|m| = \ell$.

Ejemplo 1 (Cifrado de Cesar). Sea $\mathcal{K} = \{0, 1, \dots, 9\}$, $\mathcal{M} = \{0, 1, \dots, 9\}^*$. Supongamos $m = m_0, m_1, m_2 \in \mathcal{M}$. Para cifrar m con llave k , sumamos $m_i + k \bmod 10$ para $i = 1, 2, 3$. Por ejemplo, $m = 123, k = 3 \implies c = 456$.

El cifrado de Cesar otorga secreto perfecto? No! Por ejemplo, dado $m_0 = 123$, $m_1 = 555$, $c = 567$, podemos observar que

$$\begin{aligned} \Pr[c = \text{Enc}(k, m_0)] &> 0 & (\text{existe una llave } k \text{ valida}) \\ \Pr[c = \text{Enc}(k, m_1)] &= 0. \end{aligned}$$

Una definición equivalente de secreto perfecto requiere

$$\forall m \in \mathcal{M}, c \in \mathcal{C}, \quad \Pr[M = m \mid C = c] = \Pr[M = m].$$

En nuestro ejemplo, ver $C = 567$ implica la imposibilidad de que $M = 555$, por lo cual aprendemos algo sobre M viendo C , $\Pr[M = m \mid C = c] \neq \Pr[M = m]$.

Definición 5 (One-Time Pad). Sean $n \in \mathbb{Z}_{>0}$, $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0, 1\}^n$. $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ es un one-time pad (OTP), si

$\text{Gen}()$	$\text{Enc}(k, m)$	$\text{Dec}(k, c)$
1: $k \xleftarrow{\$} \mathcal{K}$	1: $c \leftarrow m \oplus k$	1: $m' \leftarrow c \oplus k$
2: return k	2: return c	2: return m'

Teorema 3. El OTP ofrece secreto perfecto.

Proof. Sean $n \in \mathbb{Z}_{>0}$, $m_0, m_1 \in \{0, 1\}^n$, $c \in \{0, 1\}^n$.

$$\begin{aligned} \Pr_{k \sim U(\mathcal{K})} [\text{Enc}(k, m_0) = c] &= \Pr[k \oplus m_0 = c] & (\text{def. de Enc}) \\ &= \Pr[k = c \oplus m_0] \\ &= 2^{-n} & (\text{dado } k \sim U(\mathcal{K})) \\ &= \Pr[k = c \oplus m_1] \\ &= \Pr[k \oplus m_1 = c] \\ &= \Pr[\text{Enc}(k, m_1) = c]. \end{aligned}$$

□

Teorema 4 (Teorema de Shannon). Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un SKES con secreto perfecto. Entonces $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof. Por contradicción, supongamos $|\mathcal{K}| < |\mathcal{M}|$. Idea: vamos a construir m_0, m_1, c , tales que $\Pr[\text{Enc}(k, m_0) = c] > 0$ y $\Pr[\text{Enc}(k, m_1) = c] = 0$.

Fijemos $k_0 \leftarrow \text{Gen}()$, $m_0 \in \mathcal{M}$, $c = \text{Enc}(k_0, m_0)$.

$$\implies \Pr_{k \sim \text{Gen}()} [\text{Enc}(k, m_0) = c] \geq \Pr_{k \sim \text{Gen}()} [k = k_0] > 0.$$

Ahora definamos el conjunto $S := \{\text{Dec}(k, c) \mid \forall k \in \mathcal{K}\} \subset \mathcal{M}$. Notamos que $|S| \leq |\mathcal{K}| < |\mathcal{M}|$. Dado que $S \subset \mathcal{M}$ y $|S| < |\mathcal{M}|$, sabemos que $\mathcal{M} \setminus S = \{m \mid m \in \mathcal{M} \text{ y } m \notin S\} \neq \emptyset$. Elijamos $m_1 \in \mathcal{M} \setminus S$.

Supongamos que $\exists k \in \mathcal{K}$ tal que $\text{Enc}(k, m_1) = c$. Si así fuera, dado que Π es un SKES, sabemos que $\text{Dec}(k, c) = \text{Dec}(k, \text{Enc}(k, m_1)) = m_1$, lo que implicaría que $m_1 \in S$. ✗ Por lo tanto $\nexists k \in \mathcal{K}$ tal que $\text{Enc}(k, m_1) = c$

$$\implies \Pr_{k \sim \text{Gen}()} [\text{Enc}(k, m_1) = c] = 0.$$

Esto contradice la suposición que Π brinde secreto perfecto. ✗ Por lo tanto, $|\mathcal{K}| \geq |\mathcal{M}|$. □

PREGUNTA: Por que “one-time”? Alguna idea? Vamos a ver la razón próximamente.

Comentario 7. El teorema de Shannon nos dice que para obtener secreto perfecto, se requiere una llave secreta k grande al menos tanto cuanto el mensaje que se quiere ocultar. Esto nos pondría frente a la situación paradójica por la cual comunicar de manera segura un mensaje requiere comunicar de manera segura una clave no mas breve.

La única ventaja del OTP es la a-sincronía. La clave puede ser comunicada de antemano, y el mensaje determinado solo luego. Esto probablemente aun se usa en algunas embajadas.²

En la próxima clase vamos a ver nuevos postulados que nos van a permitir superar las limitaciones del teorema de Shannon.

Ataque 1 (OTP). Supongamos $\mathcal{A}$ ve $c \in \mathcal{C}$. Que aprende sobre m ? Dado cualquier $m \in \mathcal{M}$, si $k \leftarrow m \oplus c$, $\text{Dec}(k, c) = k \oplus c = (m \oplus c) \oplus c = m$. $\mathcal{A}$ solamente puede aprender que $m \in \mathcal{M}$ ($\Rightarrow$ aprende $|m|$), y que comunicación cifrada ocurrió. Usando padding extra se podría “obfuscar” $|m|$, y comunicando a intervalos regulares información “nula”, podría “obfuscarse” que la comunicación ocurrida fue significativa. Notamos que estos ataques están “fuera” de la definición de secreto perfecto, y no la contradicen.

²<https://archive.is/mmbtX#selection-1025.0-1025.238>