

Clase 15: cifrado de clave publica “one-time”

Fernando Virdia, versión: 0.1, mayo 2025

9 Cifrado de Clave Publica

Como en el caso simétrico, empezamos definiendo nociones de cifrado.

Definición 31 (PKES, cifrado asimétrico o de clave publica). Sean $\mathcal{K}_p$, $\mathcal{K}_s$, $\mathcal{M}$, $\mathcal{C}$ conjuntos. Decimos que $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ forman un cifrado asimétrico o de clave publica (PKES, “public-key encryption scheme”) con espacio de claves publicas $\mathcal{K}_p$, de claves privadas $\mathcal{K}_s$, de mensajes $\mathcal{M}$, y de cifrados $\mathcal{C}$, si

- Gen es un algoritmo aleatorio, $\text{Gen}: \emptyset \rightarrow \mathcal{K}_s \times \mathcal{K}_p$ que retorna una tupla (sk, pk) . Decimos que sk es una clave privada, o secreta, (“secret key”) y que pk es una clave publica (“public key”).
- Enc es un algoritmo (posiblemente aleatorio), $\text{Enc}: \mathcal{K}_p \times \mathcal{M} \rightarrow \mathcal{C}$.
- Dec es un algoritmo determinista $\text{Dec}: \mathcal{K}_s \times \mathcal{C} \rightarrow \mathcal{M}$.

Decimos que Π es δ -correcto si

$$\Pr_{\substack{(\text{sk}, \text{pk}) \sim \text{Gen}(), \\ \$ \text{ en Enc}}} [\text{Dec}(\text{sk}, \text{Enc}(\text{pk}, m; \$)) \neq m] \leq \delta,$$

donde Gen, Enc y Dec son “eficientes” (corren en tiempo $\approx \log_2(|m|)$).

Comentario 50. Al definir SKES, requerimos que fueran δ -correcto con $\delta = 0$. No es así con PKES, porque varias técnicas para construir PKE resulta en sistemas eficientes si $\delta \gtrsim 0$ pero menos eficientes con $\delta = 0$. En el curso vamos a ver solo sistemas con $\delta = 0$.

Comentario 51. En nuestra definición usamos conjuntos $\mathcal{M}$ y $\mathcal{C}$. En practica, es común que al generar claves, implícitamente fijemos $\mathcal{M}_{\text{pk}} \subset \mathcal{M}$ y $\mathcal{C}_{\text{pk}} \subset \mathcal{C}$ donde se encuentran los mensajes y cifrados.

Comentario 52. Diferentemente de SKE, a menudo $\mathcal{K}_s$, $\mathcal{K}_p$, $\mathcal{M}$, $\mathcal{C}$ **no son** conjuntos de cadenas de bits.

Muchas de las ideas desarrolladas para SKE pueden ser adaptadas a PKE. Una diferencia crucial es que $\mathcal{A}$ recibe pk , al ser una clave publica, y esto le permite cifrar mensajes sin requerir un oráculo.

Definición 32 (OT-IND-CPA PKE). Sea $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ un PKES.

$\text{Exp}^{\text{OT-CPA}}(\mathcal{A}, b)$	$\mathcal{O}(m_0, m_1)$
1: $(\text{sk}, \text{pk}) \leftarrow \text{Gen}()$	1: if disabled = 1 :
2: disabled $\leftarrow 0$	2: return $\perp$
3: $b' \leftarrow \mathcal{A}^{\mathcal{O}}(\text{pk})$	3: disabled $\leftarrow 1$
4: return b'	4: $c^* \leftarrow \text{Enc}(\text{pk}, m_b)$
	5: return c^*

Decimos que Π otorga one-time (ε, t) -indistinguibilidad bajo ataques de mensaje elegido (OT-IND-CPA, “one-time indistinguishability under chosen-plaintext attacks”), si cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ tiene ventaja

$$\text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{A}) := \left| \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{OT-CPA}}(\mathcal{A}, 1) \Rightarrow 1] \right| \leq \varepsilon.$$

Comentario 53. Aunque esta definición le ofrece a $\mathcal{A}$ un solo cifrado para distinguir b , a menudo la preferimos a una definición que ofrezca $q \geq 1$ cifrados. Esto es porque demostrar OT-CPA es mas fácil, y porque en el caso de PKE, $\text{OT-IND-CPA} \Rightarrow \text{IND-CPA}$.

Vamos ahora a definir el PKES de ElGamal. Puede ser visto como una versión no interactiva del KEX de Diffie-Hellman.

Definición 33 (ElGamal PKE). Sea $\mathbb{G} = (G, \times)$ un grupo cíclico generado por g . Sean $\mathcal{K}_s = [|G|]$, $\mathcal{K}_{pk} = \mathcal{M} = \mathcal{C} = G$.

Gen()	Enc(pk = g^x, m)	Dec(sk = $x, c = (c_0, c_1)$)
1: $x \xleftarrow{\$} [G]$	1: $y \xleftarrow{\$} [G]$	1: $m' \leftarrow c_1 \times c_0^{-x}$
2: $sk \leftarrow x$	2: $c_0 \leftarrow g^y$	2: return m'
3: $pk \leftarrow g^x$	3: $c_1 \leftarrow (g^x)^y \times m$	
4: return (sk, pk)	4: $c \leftarrow (c_0, c_1)$	
	5: return c	

Observamos que Π es δ -correcto con $\delta = 0$, dado que

$$m' = c_1 \times c_0^{-x} = (g^x)^y \times m \times (g^y)^{-x} = m \quad \forall x, y \in [|G|].$$

Lemma 16 (ElGamal PKE + (ε, t) -DDH $\Rightarrow$ OT-IND-CPA). Sea $\mathbb{G} = \langle g \rangle$ un grupo cíclico tal que DDH es (ε, t) -difícil. Sea Π el PKES de ElGamal definido sobre $\mathbb{G}$ con generador g . Entonces Π otorga (ε', t') -OT-IND-CPA con $\varepsilon' = 2 \cdot \varepsilon$, $t' \approx t$.

Proof. Supongamos un adversario $\mathcal{A}$ contra $\text{Exp}^{\text{OT-CPA}}$. Definimos un adversario $\mathcal{B}$ contra Exp^{DDH} .

$\mathcal{B}(g^x, g^y, g^z)$	$\mathcal{O}(m_0, m_1)$
1: disabled $\leftarrow 0$	1: if disabled = 1 :
2: $\hat{b} \xleftarrow{\$} \{0, 1\}$	2: return $\perp$
3: $\hat{b}' \leftarrow \mathcal{A}^{\mathcal{O}}(g^x)$	3: disabled $\leftarrow 1$
4: if $\hat{b}' = \hat{b}$:	4: $c^* \leftarrow (g^y, g^z \cdot m_{\hat{b}})$
5: return 0 // “ $z = x \cdot y$ ”	5: return c^*
6: else	
7: return 1 // “ $z \sim U(G)$ ”	

Recordemos la versión “bit-guessing” de $\text{Exp}^{\text{OT-CPA}}$:

$\text{Exp}^{\text{OT-CPA}}(\mathcal{A})$
1: $\hat{b} \xleftarrow{\$} \{0, 1\}$
2: $\hat{b}' \leftarrow \text{Exp}^{\text{OT-CPA}}(\mathcal{A}, \hat{b})$
3: return $[\hat{b}' = \hat{b}]$

Usando la misma demostración de Lemma 3, sabemos que

$$\text{Adv}(\overline{\text{Exp}^{\text{OT-CPA}}}, \mathcal{A}) := \left| \Pr[\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| = \frac{1}{2} \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{A}).$$

Por inspección, podemos ver que el entorno de $\mathcal{A}$ en $\text{Exp}^{\text{DDH}}(\mathcal{B}, 0)$, es idéntico al de $\mathcal{A}$ en $\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A})$ si $pk = g^x$ y $c_0^* = g^y$. Por ende,

$$\begin{aligned} \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] &= \Pr[\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 0] = 1 - \Pr[\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] \\ \iff \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} &= \frac{1}{2} - \Pr[\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] \\ \iff \text{Adv}(\overline{\text{Exp}^{\text{OT-CPA}}}, \mathcal{A}) &= \left| \Pr[\overline{\text{Exp}^{\text{OT-CPA}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| = \left| \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} \right|. \end{aligned}$$

Dentro de $\text{Exp}^{\text{DDH}}(\mathcal{B}, 1)$, $\mathcal{A}$ recibe $(g^x, g^y, g^z \cdot m_{\hat{b}})$, donde $g^z \sim U(\mathbb{G})$, independientemente de (g^x, g^y) . Por lo tanto, la vista de $\mathcal{A}$ es independiente de $\hat{b}$, dado que

$$\Pr[h = g^z \cdot m_0] = \Pr[g^z = h \cdot m_0^{-1}] = \frac{1}{|\mathbb{G}|} = \Pr[g^z = h \cdot m_1^{-1}] = \Pr[h = g^z \cdot m_1]$$

Al ser el valor $\hat{b}'$ retornado por $\mathcal{A}$ independiente de $\hat{b}$, y al ser $\hat{b} \sim U(\{0, 1\})$, sigue que

$$\Pr[\hat{b}' \neq \hat{b}] = \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 1) \Rightarrow 1] = \frac{1}{2}.$$

Finalmente,

$$\begin{aligned} \text{Adv}(\text{Exp}^{\text{OT-CPA}}, \mathcal{A}) &= 2 \cdot \text{Adv}(\overline{\text{Exp}^{\text{OT-CPA}}}, \mathcal{A}) \\ &= 2 \cdot \left| \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \frac{1}{2} \right| \\ &= 2 \cdot \left| \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{DDH}}(\mathcal{B}, 1) \Rightarrow 1] \right| \\ &= 2 \cdot \text{Adv}(\text{Exp}^{\text{DDH}}, \mathcal{B}). \end{aligned}$$

Claramente, $t' \approx t$, $\varepsilon' = 2 \cdot \varepsilon$, y Π ofrece $(2\varepsilon, \approx t)$ -OT-IND-CPA. □