

Clase 6: cifrados de bloque

Fernando Virdia, versión: 0.1, mayo 2025

Definición 14 (PRP). Sean $\mathcal{K}, \mathcal{D}$ dos conjuntos finitos. Sea $\pi: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{D}$ una función, tal que $\forall k \in \mathcal{K}, \pi(k, \cdot): \mathcal{D} \rightarrow \mathcal{D}$ tiene una inversa $\pi^{-1}(k, \cdot): \mathcal{D} \rightarrow \mathcal{D}$ (tal que $\forall x \in \mathcal{D}, \pi(k, \pi^{-1}(k, x)) = \pi^{-1}(k, \pi(k, x)) = x$). Sean π y π^{-1} implementables como algoritmos deterministas eficientes.

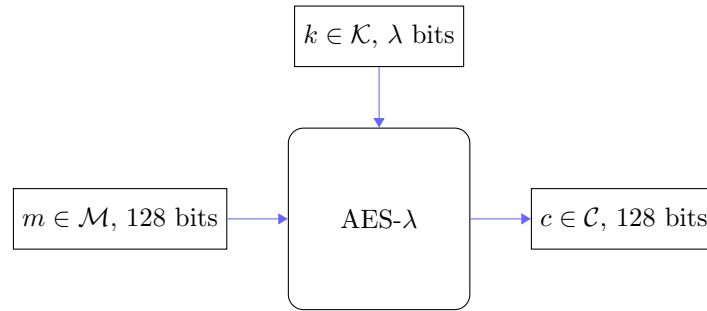
$\text{Exp}^{\text{PRP}}(\mathcal{A}, b)$	$P(x)$	$\mathcal{O}(x)$
1: $k \xleftarrow{\$} \mathcal{K}$	1: if $x \notin L$:	1: if $b = 0$
2: $L \leftarrow []$	2: $y \xleftarrow{\$} \mathcal{D} \setminus \{L[x] \mid \forall x \in L\}$	2: $y \leftarrow \pi(k, x)$
3: $b' \leftarrow \mathcal{A}^{\mathcal{O}(\cdot)}()$	3: $L[x] \leftarrow y$	3: else
4: return b'	4: return $L[x]$	4: $y \leftarrow P(x)$
		5: return y

Decimos que π es una familia de permutaciones (ε, t, q) -pseudoaleatoria indexada por $k \in \mathcal{K}$ (PRP, “pseudorandom permutation family”), o un cifrado de bloques, si dado cualquier adversario $\mathcal{A}$ que corre en tiempo $\leq t$ y hace $\leq q$ queries a $\mathcal{O}(\cdot)$, tiene ventaja

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

Comentario 20. Una permutación π con $\mathcal{D} = \{0, 1\}^d$ permuta cadenas en $\mathcal{D}$, no bits en una cadena. Por ejemplo, dado $d = 3$, $\pi(k, 010)$ podría ser 111, aunque estas cadenas tengan diferentes números de bits = 1.

Comentario 21. Por motivos históricos y prácticos, los algoritmos de cifrado de bloque, o PRP, son entre los componentes mas usados (correctamente y no) y estudiados de la criptología. Hoy en día, el mas utilizado es el Advanced Encryption Standard (AES), que tolera $\mathcal{D} = \{0, 1\}^{128}$ y presenta tres variantes: AES-128, con $|k| = 128$, AES-192, con $|k| = 192$, AES-256, con $|k| = 256$. Se estima que AES- λ ofrece $\lambda = \log_2(t/\varepsilon)$ bits de seguridad (ε, t, q) -PRP.



Los algoritmos de cifrado de bloque se utilizan a menudo en “modos de operacion”. Pueden haber oído de ECB-mode (un modo prácticamente siempre inseguro), CBC-, CTR-, GCM-... No vamos a estudiar todos estos, dados que a menudo pensar en términos de modos de operación, en lugar que en términos de modelos de seguridad, puede resultar en la introducción de vulnerabilidades en protocolos. En efecto, vamos a cubrir métodos equivalentes al CTR y GCM.

PRGs, PRFs y PRPs son equivalentes, o sea:

- PRP $\Rightarrow$ PRF: “PRP-PRF switching lemma”
- PRF $\Rightarrow$ PRP: “Feistel networks”
- PRF $\Rightarrow$ PRG: $F(k, x_1) || \dots || F(k, x_q)$
- PRG $\Rightarrow$ PRF: “GGM”

Definición 15 (λ -bits de seguridad bajo q queries). Sea Π una primitiva criptografica, y sea “X” una nocion de seguridad con experimento Exp^X , que le otorga al adversario q queries a un oraculo. Supongamos que existe $\lambda \in \mathbb{Z}_{>0}$ tal que para cualquier $\varepsilon \in [0, 1]$, Π otorga (ε, t, q) -X-seguridad con $t \geq 2^\lambda \cdot \varepsilon$. Entonces decimos que Π otorga λ bits de X-seguridad bajo q queries.

En el resto del curso, usaremos este postulado.

Postulado 2. *Dados $q, \lambda \geq 0$, existe un cifrado de bloque Π que otorga λ -bits de seguridad PRP bajo q queries.*

Completamos este tema, construyendo PRFs de PRPs, y PRGs de PRFs.

De PRP a PRF.

La idea de esta construcción es que una PRP es una PRF, si $\mathcal{A}$ observa pocos outputs. Para demostrarlo, primero vemos dos lemas requeridos.

Lemma 5 (Difference lemma, lema de la diferencia). *Sean E_1, E_2, Z tres eventos donde*

$$E_1 \wedge \bar{Z} \iff E_2 \wedge \bar{Z}.$$

Entonces $|\Pr[E_1] - \Pr[E_2]| \leq \Pr[Z]$.

Comentario 22. “Si se necesita Z para distinguir E_1 de E_2 , la probabilidad de distinguirlos es al máximo la probabilidad de que Z suceda.”

Proof. Calculamos

$$\begin{aligned} |\Pr[E_1] - \Pr[E_2]| &= |(\Pr[E_1 \wedge Z] + \cancel{\Pr[E_1 \wedge \bar{Z}]}) - (\Pr[\cancel{E_2 \wedge Z}] + \Pr[E_2 \wedge \bar{Z}])| \\ &= |\Pr[E_1 \wedge Z] - \Pr[E_2 \wedge Z]|. \end{aligned}$$

Dado que $0 \leq \Pr[E_i \wedge Z] \leq \Pr[Z]$, con $i = 1, 2$,

$$\implies |\Pr[E_1 \wedge Z] - \Pr[E_2 \wedge Z]| \leq \Pr[Z].$$

□

Lemma 6 (Birthday bound, paradoja del cumpleaños). *Dados $q \in \mathbb{Z}_{>0}$, $\mathcal{R}$ un conjunto finito, y $z_1, \dots, z_q \in \mathcal{R}$ muestreados $z_i \sim U(\mathcal{R})$ de manera independiente,*

$$\Pr[\exists i, j \in [q] : i \neq j \wedge z_i = z_j] \leq \frac{q(q-1)}{2|\mathcal{R}|}$$

Proof. Calculamos

$$\begin{aligned} \Pr[\exists i, j \in [q] : i \neq j \wedge z_i = z_j] &= \Pr \left[\bigvee_{i \neq j} z_i = z_j \right] \\ &\leq \sum_{i \neq j} \Pr[z_i = z_j] \quad (\text{por la cota de la unión}) \\ &= \sum_{i \neq j} \frac{1}{|\mathcal{R}|} = \binom{q}{2} \frac{1}{|\mathcal{R}|} = \frac{q(q-1)}{2|\mathcal{R}|}. \end{aligned}$$

□

Comentario 23. *El birthday bound es una cota superior “tight” o “ajustada”, o sea que el valor efectivo de la probabilidad de colisión es muy cercano a la cota. Efectivamente, también se puede demostrar una cota inferior muy cercana, de $\approx \frac{q(q-1)}{4|\mathcal{R}|}$ [KL20, Lemma A.15].*

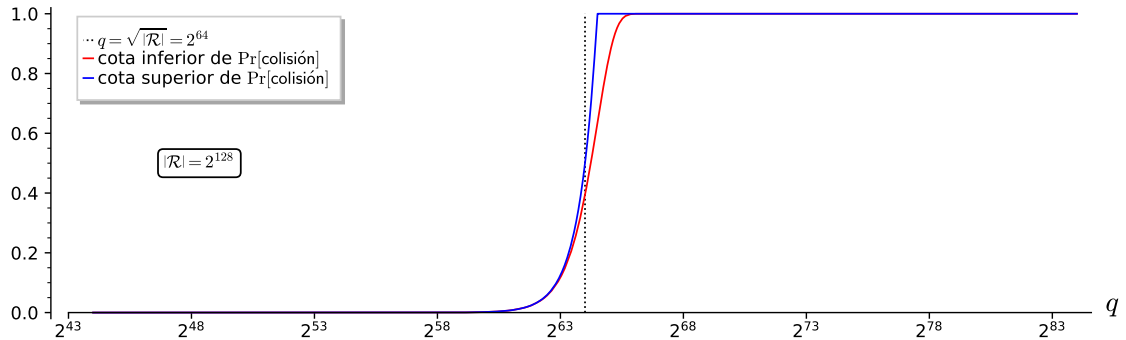


Figure 3: Visualizando las cotas en función de q , vemos que la probabilidad “salta” de ≈ 0 a ≈ 1 alrededor de $q = \sqrt{|\mathcal{R}|}$.