

¿Y si ciframos con atributos?

Jose María de Fuentes
jfuentes@inf.uc3m.es

12 de febrero de 2026

1. El cifrado basado en Atributos

El cifrado basado en atributos (Attribute-Based Encryption, ABE) es un esquema en el que el acceso a los datos se controla por atributos (p. ej. rol, departamento, nivel) en lugar de por identidad concreta. En ABE se cifra bajo una política de atributos y solo las claves que cumplen esa política pueden descifrar.

Dos familias principales

- Key-Policy ABE (KP-ABE):
 - El emisor etiqueta el texto cifrado con un conjunto de atributos.
 - La clave privada incorpora una política (por ejemplo: $((A \text{ AND } B) \text{ OR } C)$); solo si los atributos del texto cifrado satisfacen la política, se puede descifrar.
- Ciphertext-Policy ABE (CP-ABE):
 - El emisor especifica la política en el texto cifrado.
 - Las claves privadas están asociadas a un conjunto de atributos del usuario.
 - Si los atributos del usuario satisfacen la política del texto cifrado, puede descifrar.

Componentes básicos (CP-ABE, esquema típico)

- $\text{Setup}(\lambda) \rightarrow$ genera PK (parámetros públicos) y MSK (master secret key).
- $\text{KeyGen}(\text{MSK}, S) \rightarrow$ con $S =$ conjunto de atributos del usuario $\rightarrow$ genera SK_S .
- $\text{Encrypt}(\text{PK}, M, \text{policy}) \rightarrow$ cifra M bajo una política $\rightarrow$ produce CT.
- $\text{Decrypt}(\text{SK}_S, \text{CT}) \rightarrow$ si S satisface policy, devuelve M ; si no, fallo.

2. El Reto

Implementa, en el lenguaje de programación que desees, un sistema CP-ABE con atributos, que son etiquetas simples (sin operadores numéricos), para cifrar documentos en entornos médicos:

- Atributos disponibles en el sistema: doctor, cardiology, senior, research.
- Por ejemplo, los documentos pueden ser cifrados con políticas del tipo: (doctor AND cardiology) OR (senior AND research).

Posteriormente implementa el mismo sistema con cifrado simétrico, por ejemplo, cifrando los documentos con AES, y analiza el rendimiento (en términos de cómputo) y las ventajas y las desventajas frente a ABE.