Asunciones de seguridad

Asunciones de seguridad

El cifrado de información no previene la interceptación de la comunicación → El atacante tiene acceso a todos los textos cifrados utilizando el criptosistema

El criptosistema no garantiza confidencialidad de extremo a extremo → El atacante puede tener acceso a determinados pares de texto plano y texto cifrado

El criptosistema suele ser público → El atacante conoce los detalles del algoritmo de cifrado/descifrado

Segundo principio de Kerckhoffs

“La efectividad del sistema no debe depender de que su diseño permanezca en secreto” [1]

Un algoritmo criptográfico público tiene más probabilidades de haber sido estudiado por un número mayor de expertos

Presenta mayor compatibilidad con un rango más amplio de tecnologías

Proporciona mayor transparencia para los *stakeholders* que quieran conocer su robustez

[1] Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5–38 "II. DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.", Jan. 1883