Perfect secrecy

Perfect secrecy

El conceto *perfect secrecy* describe un **criptosistema que no se puede romper**

Decimos que un criptosistema tiene *perfect secrecy* si después de que un **atacante intercepte texto cifrado no puede obtener información adicional sobre el texto plano** a la que ya tenía antes de interceptarlo

En un criptosistema que tiene *perfect secrecy* la mejor estrategia de un atacante en intentar adivinar el texto plano

Perfect secrecy | Ejemplo práctico

	COMPRAR	**VENDER**
Clave K_1	Ek_1(COMPRAR) = 0	Ek_1(VENDER) = 1
Clave K_2	Ek_2(COMPRAR) = 1	Ek_2(VENDER) = 0