Uso de One-time pads

Uso de One-time pads

La longitud de la clave provoca que no sea práctico para muchas aplicaciones

La clave debe ser generada de manera realmente aleatoria. Este proceso es muy costoso.

Que la clave sea de un solo uso acentúa los problemas expuestos en los dos puntos anteriores e invalida su implementación práctica

El uso de one-time pads puede tener sentido en entornos de muy alta seguridad o para cifrar mensajes muy cortos

Uso de One-time pads

¿Esto quiere decir que teóricamente todos los criptosistemas que se utilizan en la actualidad se pueden romper?

En la práctica, los criptosistemas modernos son tan seguros como los *one-time pads* porque los ataques teóricos existentes requieren un número demasiado elevado de recursos para llevarlos a cabo