

# ¿Como funciona el cifrado en las apps de mensajería instantánea?

La hija de la familia Cibernauta está chateando con su mejor amiga. Mientras, los ciberdelincuentes tratan de interceptar estos mensajes, pero ¿es eso posible?

Las aplicaciones de mensajería más populares utilizan cifrado de extremo a extremo.



Al **cifrar y descifrar** los mensajes, se emplean **dos tipos de clave**:

## Clave pública:

Es la que **deberemos compartir con el receptor** para que cifre con ella el mensaje que nos va a enviar.



## Clave privada:

Nos **permitirá descifrar y leer el contenido** del mensaje recibido.

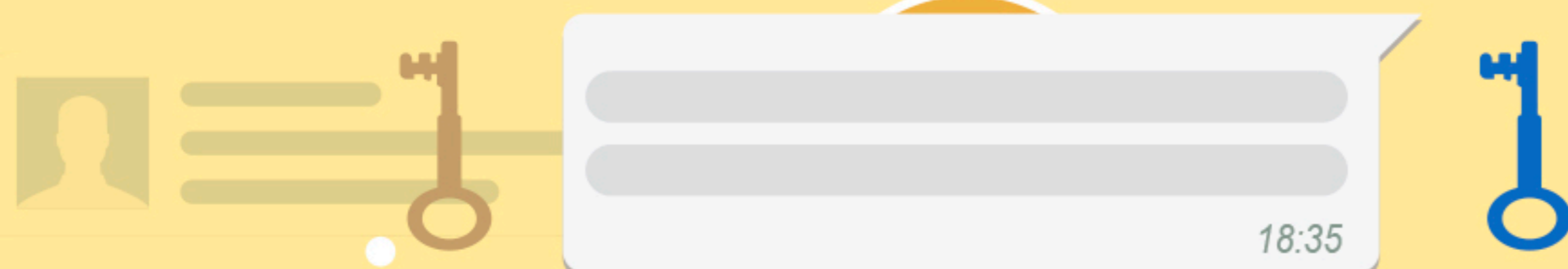


Hola, ¿qué tal? ¡no me has enviado las fotos del finde aún!

18:35

Enviado ✓

Este **mensaje se cifra con la clave pública** del receptor (amiga). **Y se firma con la llave privada** del usuario (hija).



El mensaje se envía firmado y cifrado. **Sin las claves, es ilegible.**

El mensaje se valida con la llave pública del que envía (hija) y se **descifra con la llave privada** del receptor (amiga).

Leído ✓✓



Con este mecanismo **nadie puede descifrar el mensaje**, salvo el autor y la persona a la que está dirigida. **¡Nadie más!**

Este tipo de cifrado es utilizado por aplicaciones de mensajería instantánea tan famosas como **Whatsapp** y permite incluso cifrar el contenido de las llamadas, los grupos y el envío de imágenes.

