¿Cómo funcionan las llaves públicas y privadas?

Siempre un tema complicado, pero hay una forma bastante simple de explicarlo. Empecemos con el ciframiento convencional.

Digamos que tengo que enviar una información importante pero no puedo confiar en el mensajero. Por lo tanto, escribo mi mensaje en un papel, lo meto en una caja de metal, le pongo un candado y lo envío. La caja llega a su destino sin problema, pero el destinatario no puede leerla, pues no puede abrir el candado. Si le envío la llave, aunque sea por otro medio -otro mensajero-, puede verse que hay un nivel de riesgo, al comprometer la seguridad de la llave, confiándola a extraños. Así funciona el ciframiento convencional.

Cambiemos ahora un poco la situación. Digamos ahora que el destinatario me envía previamente un candado, abierto. Es “su” candado, yo no puedo abrirlo si se cierra, pues la llave solamente la tiene él. La llave permanecerá segura en su poder. Recibo el candado, escribo mi mensaje, lo meto en la caja y cierro la caja con el candado que recibí. A partir de ese momento, ni yo mismo, que escribí el mensaje, puedo ya verlo. Está protegido por el candado. Envío la caja y el destinatario la abre con su llave. Así funciona la llave pública y privada. La llave pública es el candado y su pareja es la llave de metal (llave privada) que lo abre. Por supuesto, esta pareja debe ser fabricada una para la otra.

La versión criptográfica es un par de secuencias de caracteres, que usadas por un programa adecuado pueden cifrar y descifrar un texto. La llave pública solamente puede cifrar. La llave privada puede descifrar, o hacer las dos cosas, aunque esto último no es tan importante. Yo recibo la llave pública de mi destinatario y con ella cifro la información que le enviaré. Una vez cifrada, yo mismo no puedo ver la información. Envío esta información, en un correo, por ejemplo, el destinatario la recibe y la descifra con su llave privada.

No hay peligro en publicar las llaves públicas porque son precisamente para eso. Y están diseñadas de manera que es muy difícil -casi imposible con la tecnología actual- deducir una llave privada de una pública. Y claro, ambas llaves deben ser generadas previamente, como un par correspondiente, igual que el candado y su llave.