Correo Electrónico Seguro – Cifrado

El cifrado del correo electrónico nos permite proteger el contenido, impidiendo ser leído por terceros, así como asegurar la autenticidad y el origen de procedencia.

El cifrado del correo electrónico dispone de dos claves, una pública y otra privada; la pública será conocida por todos los usuarios con los que nos comuniquemos, y la privada que es conocida única y exclusivamente por el interesado.

EJEMPLOS, donde **A es el emisor y B es el receptor** de los mensajes:

1) A quiere enviar información a B, y que solo él pueda leer. Deben realizarse los siguientes pasos:
   - A cifra el mensaje con la clave pública de B (que todos conocen).
   - Solo B podrá descifrar el mensaje con su clave privada (que solo él conoce).

   En esta situación aseguramos que la información solo la puede ver B, pero no se puede garantizar que el remitente sea A.
2) A quiere enviar información a B (en este caso son varios receptores), de forma que se garantice que la información es de A. En este caso:
   - A cifra la información con su clave privada (que solo él conoce).
   - B puede descifrar la información con la clave pública de A (que todos conocen), y como solo A conoce su clave privada se garantiza también su origen.
3) A quiere enviar información a B, de forma que garantice que la información es de A y que solo B la pueda leer. En este caso haremos una combinación de las dos anteriores:
   - A cifra con su clave privada que garantiza que es su mensaje, y con la clave pública de B para que solo él pueda leerlo.
   - B descifra con la clave pública de A garantizando así el remitente, y con su clave privada garantizando que solo él puede leer el mensaje.

La aplicación práctica de todo esto se conoce con el nombre de protocolo PGP Pretty Good Privacy.
En Windows podemos utilizar herramientas como GPG4win.
En Mac podemos utilizar GPG suite y GNUPG para Linux/Mac.

Estas herramientas se encargan automáticamente de generar las claves pública y privada integrándose en el propio correo electrónico. [1]

[1] https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/incibe_cert_guia_para_el_uso_de_pgp_en_clientes_de_correo_electronico.pdf
Mailvelope extensión para Firefox y Google Chrome que permite cifrar nuestros correos
https://www.mailvelope.com/es/help