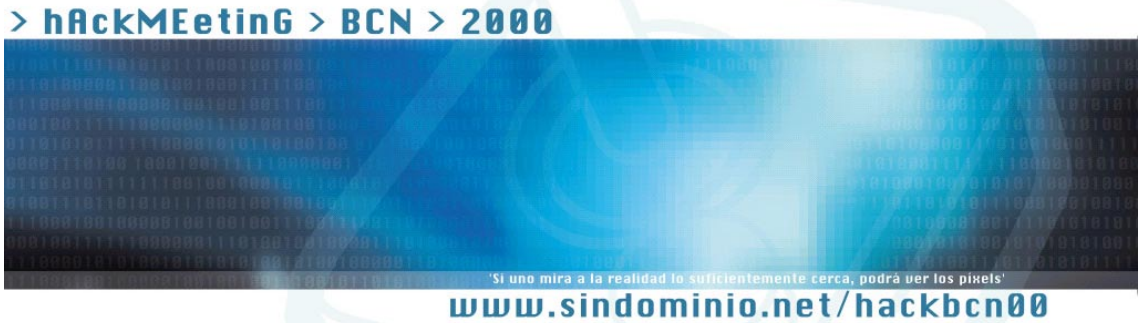
Cifrado de correo para novat@s



Alejandro Castán Salinas

alex.castan@upc.es

¿Qué es el cifrado?

Cifrar un mensaje consiste en alterar el contenido de dicho mensaje de tal manera que tan sólo las personas a quienes vaya dirigido el mensaje podrán descifrarlo, siempre que conozcan el sistema de cifrado y la clave necesarios.

¿Qué es la firma?

Firmar un mensaje consiste en añadir una marca al final de mensaje de tal manera que las personas que lo reciban puedan comprobar que el mensaje proviene de la fuente correcta y que éste no ha sido modificado para falsear su contenido original.

¿Por qué cifrar o firmar?

Cuando enviamos una carta por correo cerramos el sobre para que no lea el mensaje nadie más que el destinatario. Muy pocas veces lo hacemos porque se trate de un mensaje secreto. La mayoría de veces lo hacemos sencillamente porque queremos preservar nuestra intimidad. A nadie le gusta que otras personas para las que no iba destinado el mensaje lean lo que uno siente, piensa, hace, dice, etc.

De la misma manera, al final de una carta añadimos nuestra firma para que la persona que la reciba pueda comprobar que realmente lo hemos escrito nosotros.

Cuando enviamos un mensaje de correo electrónico por Internet, todos los ordenadores intermedios por los que circula dicho mensaje pueden interceptar, leer, procesar, almacenar o modificar el mensaje. Sin embargo, normalmente no somos conscientes del peligro y de la invasión de nuestra intimidad que ello supone.

Existen programas especiales que nos permiten cifrar y firmar tanto nuestro correo electrónico como nuestros ficheros en un ordenador, para preservar nuestra intimidad y la autenticidad de éstos.

Programas de cifrado

Existen numerosos métodos de firma y de cifrado de información: DES, RSA, Diffie-Hellman, Twofish, Rijndael, etc. No entraremos en detalle de como funcionan. Tan solo nos basta saber que los programas de cifrado nos permiten utilizar dichos métodos para codificar el mensaje a enviar y descodificar el mensaje recibido. De esta manera tan sólo tenemos que escribir el mensaje de correo electrónico y utilizar alguno de estos programas para cifrar el mensaje con una clave tal que tan sólo la persona destinataria del mensaje podrá descifrarlo si posee la clave adecuada. Si además queremos firmarlo, el programa de cifrado añadirá un texto a final del mensaje elaborado a partir de dicho mensaje y una clave nuestra, que permitirá comprobar que dicho mensaje lo enviamos nosotros y no fue modificado por el camino.

Es importante tener claro que no hace falta que la persona emisora del mensaje y la persona receptora del mensaje utilicen el mismo programa de cifrado, pero sí que utilicen el mismo método.

Para comenzar, los programas de cifrado gratuitos más sencillos que he encontrado en Internet son:

- Para los usuarios de Windows recomiendo PGP. Es un programa completo y fácil de manejar, con una interfície gráfica clara e intuitiva. Se integra perfectamente en el entorno de trabajo añadiendo menús contextuales e iconos en los programas de correo más habituales. También está disponible para otros sistemas operativos. Se puede encontrar en http://www.pgpi.org.

- Para los amantes del código abierto recomiendo GnuPG. Esta disponible para una gran variedad de sistemas operativos en http://www.gnupg.org, aunque los binarios RPM de fácil y rápida instalación se encuentran en ftp://crypto.ferrara.linux.it/pub/gpg/. GnuPG es un programa que se utiliza desde la línea de comandos, pero se puede añadir una interfície gráfica para poder utilizarlo de una manera cómoda. Una de las interfícies gráficas más sencillas que he encontrado es Seahorse para Gnome en http://seahorse.sourceforge.net/. El mismo equipo de GnuPG está desarrollando la interfície gráfica "oficial" llamada GPA que se encuentra en http://www.gnupg.org/gpa.html.
- Como curiosidad, dozeCrypt! es un pequeño programa (cabe en un disquete) que no necesita instalación y que permite fácilmente cifrar y descifrar ficheros mediante doce métodos diferentes. Especialmente recomendado para las personas que trabajan con ordenadores ajenos (en cibercafés, etc.). Se puede conseguir en http://www.neuralabyss.com/dozecrypt/.

Una vez hemos instalado en nuestro ordenador el programa de cifrado, el primer paso es generar nuestro par de claves. Se trata de generar una clave que llamamos "pública" que utilizará la gente para cifrarnos los mensajes, y otra clave que llamamos "privada" que, previa introducción de una contraseña de acceso, tan solo utilizaremos nosotros para firmar mensajes y para descifrar los mensajes que nos hayan enviado. Cuanto mayor sea la longitud de las claves, más tardarán en generarse, pero también mayor será la seguridad que nos ofrecerán. La clave pública la podemos colgar de un servidor de claves públicas para que esté disponible para todo el mundo en Internet, y también la podemos enviar como fichero adjunto en los mensajes a nuestros amigos y amigas.

El siguiente paso será añadir a nuestra colección de claves las claves públicas de todas aquellas personas a quienes escribimos mensajes cifrados y que queremos tener permanentemente almacenadas.

A partir de este punto ya podemos cifrar/descifrar y firmar/comprobar tanto correo electrónico como ficheros.

Cursos de cifrado

Por cuestión de falta de tiempo, no puedo elaborar el curso de cifrado para PGP y GnuPG. Sin embargo, ya existen dos cursos breves y excelentes en http://kriptopolis.com/pgp/ (PGP) y http://kriptopolis.com/gpg/ (GnuPG).

También existen numerosos manuales tanto de GnuPG como de PGP disponibles en Internet. Podéis comenzar a buscar en http://www.pgpi.org/doc/, http://www.gnupg.org/gph/es/ y http://www.kriptopolis.com.

Llave pública del autor

Por si alguien decide enviarme algún mensaje, aquí tenéis mi clave pública. Ya podéis comenzar a practicar ;-)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>

mQGiBDgq7lsRBADhzCLFlA6HrbxHO0fOSw6n2qPHCHeus/Q4LmOgv2O+F2MwAYjN
vY9CW6lljuGEtesrFAPwgr0kJvacn6yF3gfSyvsAmzL7YBN6k4soFM3sZFBEdTIm
g7QX14S03QBFlOu0DEcxvil8SrTruTFJp0/fn6ZJZLUZqPY8g8C9znfCWwCg/97Z
xh8M2N0HYrU2a4tlc+htdccEAK5VDTCO3iawab340fc+wGRS3hHGRYgfpDLeZ8Cc
pRh17XgPe+H3fsiO0vTqPinsES+y4c9kIkjcvAMZxZ9Pj/UOsyTNETmKaBuJnO6C
rdU+77UvlTlqZjmT93Tdr90LhEYveW3qMFRwTDfV8wCcuIrHqo9xBLaoBc3nS5fx
axM2BACvyCk8O8GNoTet59khaukcwfidRVEGhew6gz2zi/fEOSSTZdGbjsbDTuHH
lKr0SI/pr7ZVwqt2WjJagiZw4/IBCbq53KgjHnNNVrhqYluu5Xx4fhsAPyqAnUWi
8ljAyU3Jd6/qeB7e+1pWRdYmLyLSV4oNVMX2gU1n//uclv2RhbQzQWxlamFuZHJv
IENhc3ThbiBTYWxpbmFzIDxhY2FzdGFuQGl0LmV1ZXRpYi51cGMuZXM+iQBOBBAR
AgAOBQI4Ku5bBAsDAgECGQEACgkQ0ylMK2M/N6JDYgCg1riz1qXq+E1MIUo5R3Xf
sKr9lVwAn3g8N4nh8V2m5bCYg+2+JAuPJz7PuQMNBDgq7l0QDADMHXdXJDhK4sTw
6I4TZ5dOkhNh9tvrJQ4X/faY98h8ebByHTh1+/bBc8SDESYrQ2DD4+jWCv2hKCYL
rqmus2UPogBTAaB81qujEh76DyrOH3SET8rzF/OkQOnX0ne2Qi0CNsEmy2henXyY
CQqNfi3t5F159dSST5sYjvwqp0t8MvZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65
Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09
jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brw
v0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiN
jrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK
lQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVelMMm8AAgIL/2THCIUJ
7tkUZUgqyd0bJybVyhc9Vkn10393RReC/rVBnsaQ9SpLHH8l03ArTY262GKRJ2cA
DJKDyn8cpIkU6f/SOKA79y3ruTZLrx4l80K2vZ1dbHnLEK95f0HYnmrHSWMSmxEg
4r86gperdjY2fezbubeb6wfSaqqe4Bx3WDF3woQMCRIhvmpt2WE4puonHrnbBHOE
rUye9Tc0skuLzdQEjN9porUVtiDNE5kk29obN2Ai6rvp1/Zcu6T+DMLizQiTkOWS
QDL5e0ZLF/kvgQtc1LhopH9nLCIzOP8S921phKlxLNO+vU2UeUuExmLgDlW+ofqR
z+HyxHpxn2/VecLCHNzklgsWWSOQ8n5pQ0K6MhbjGt/UQwrKly8qvDrEwSpYByle
5BGBEaTJVT4Bg9Q575E+N47vp7mXfJahdQXgXjjHppcoM/pDscaqC2hWRGa0T7CN
AZ1CsjQqyUKrvht6l7lLzj7bF6pvxQyKErZB/eeHSCjFlT/t9wil5TxOWIkARgQY
EQIABgUCOCruXQAKCRDTKUwrYz83omuVAJ9NKnlO1qCSz/TySMGCPmYy0S+eTQCe
JRc8LL8ZxfjEMLptgIcRvnNea6Q=
=Dgp9
-----END PGP PUBLIC KEY BLOCK-----
```