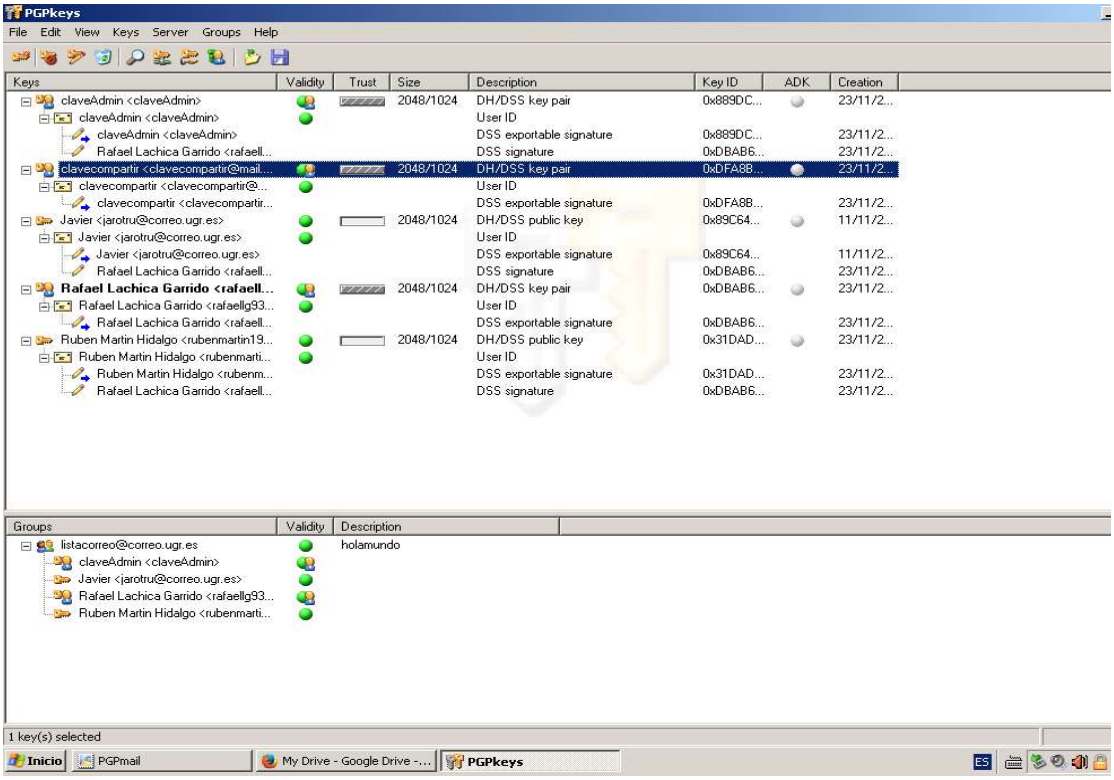
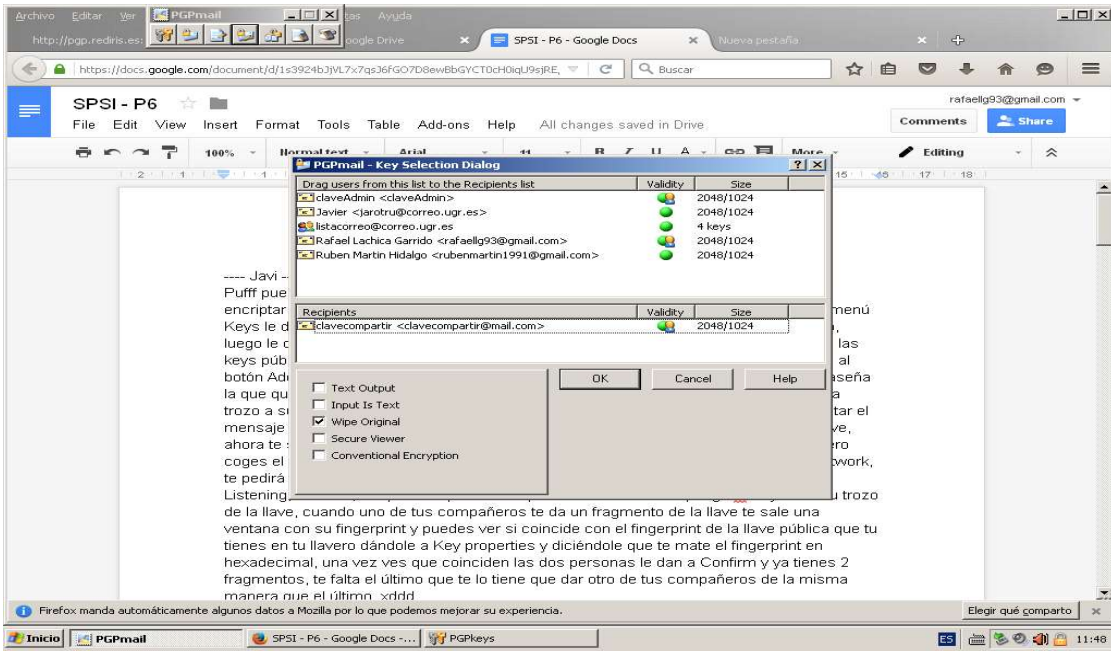
PRÁCTICA 6

SHARE SPLIT KEY

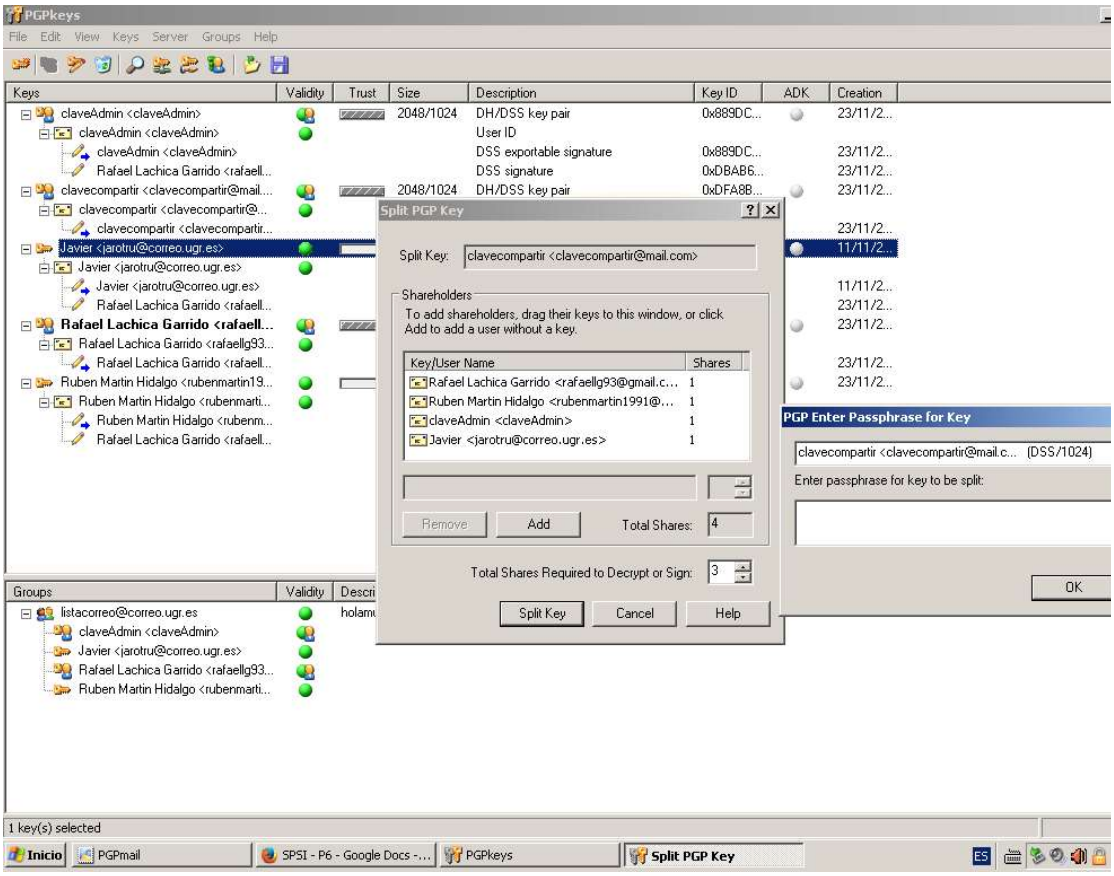
Imagen con todas las claves



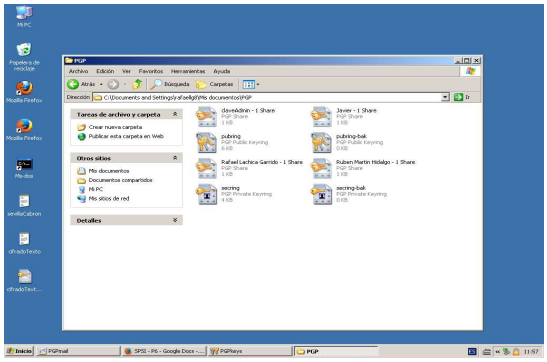
Encriptamos un mensaje con la clave a compartir y borramos el original:

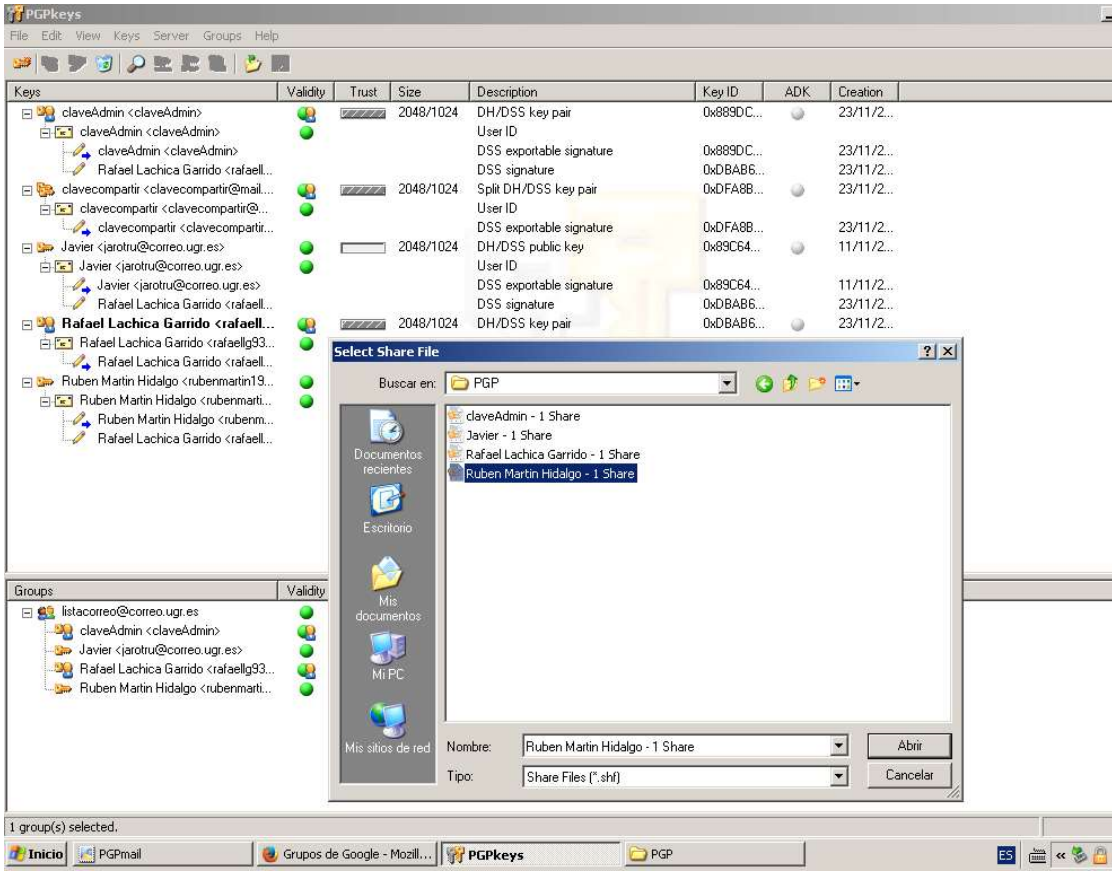


Partimos la clave entre 4 sombras, pero podemos desencriptar con solo 3:

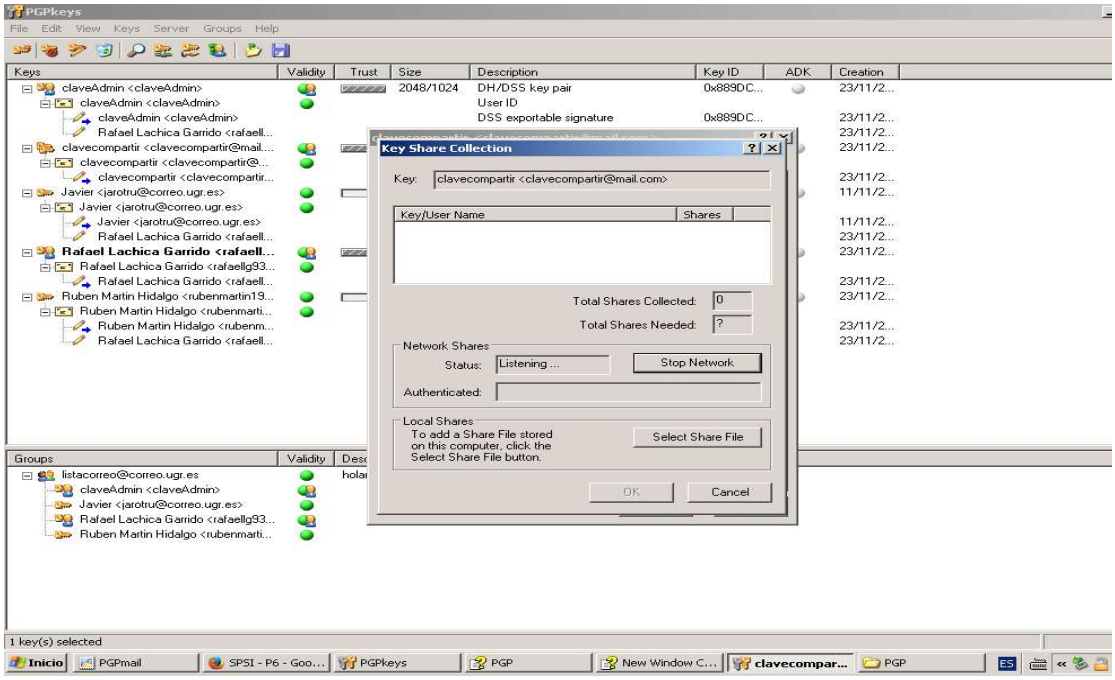


Repartimos los shares:
Enviamos a cada usuario su clave de esta carpeta correspondiente a través de la lista de correo:

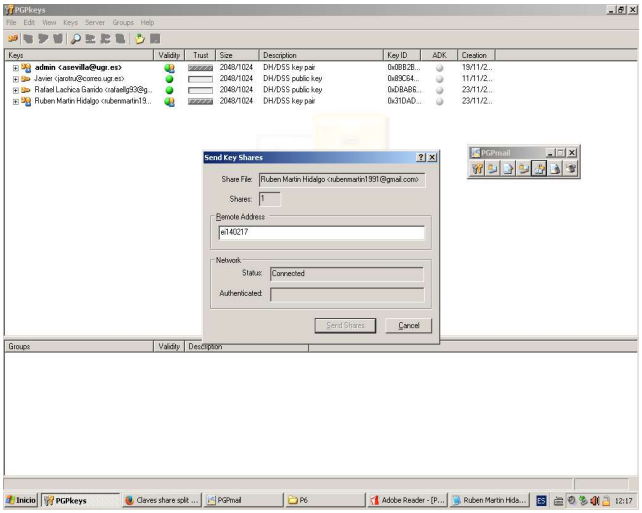


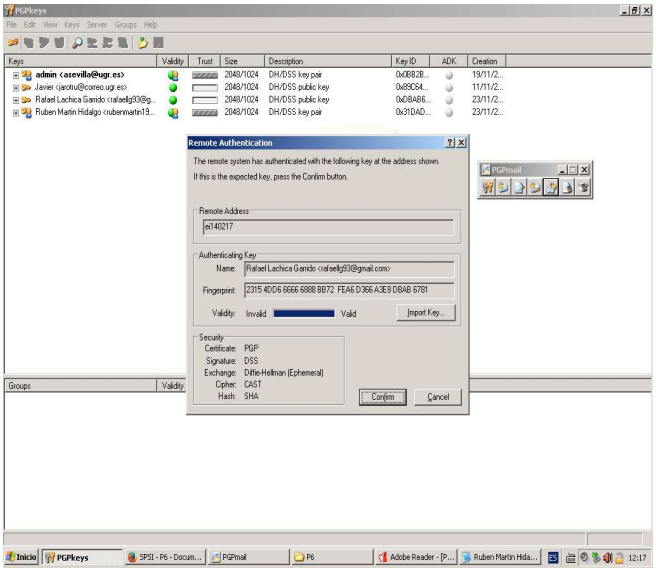


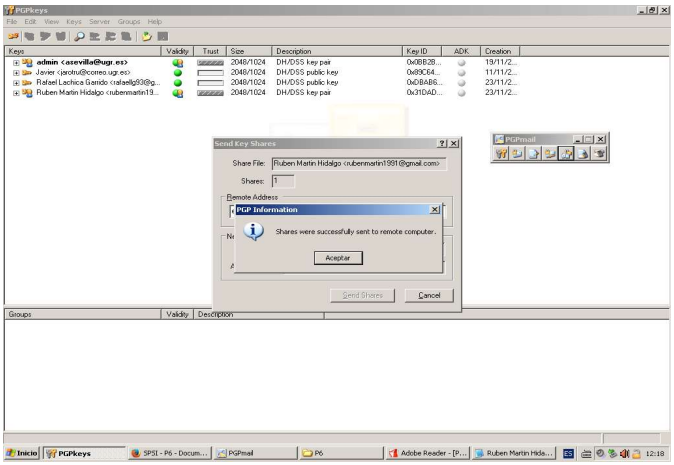
Después de mandarlo por correo para reunir las claves para desencriptar obtenemos las claves del servidor que está escuchando:



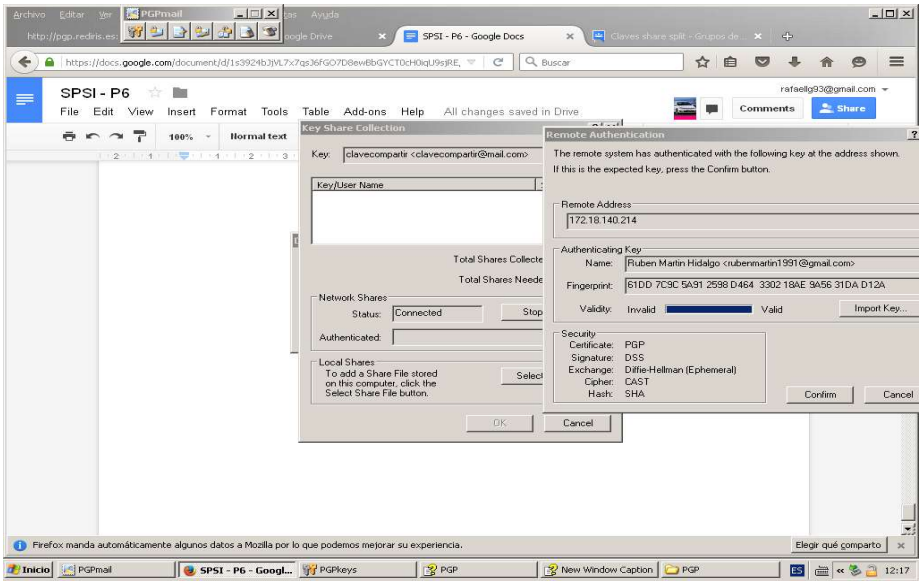
Ahora envía cada usuario su share a través de “File -> Send Key Shares”, mientras el admin está escuchando:



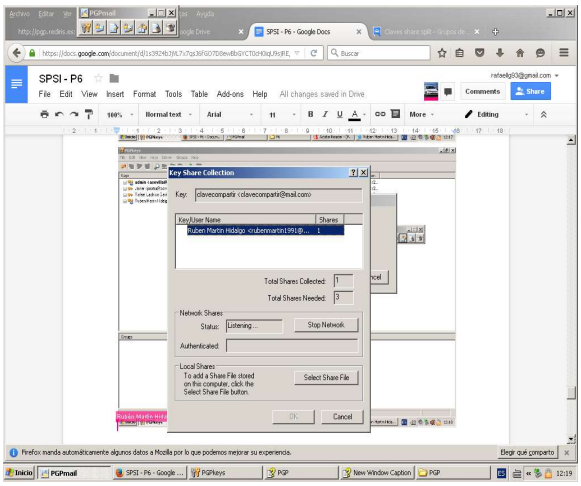




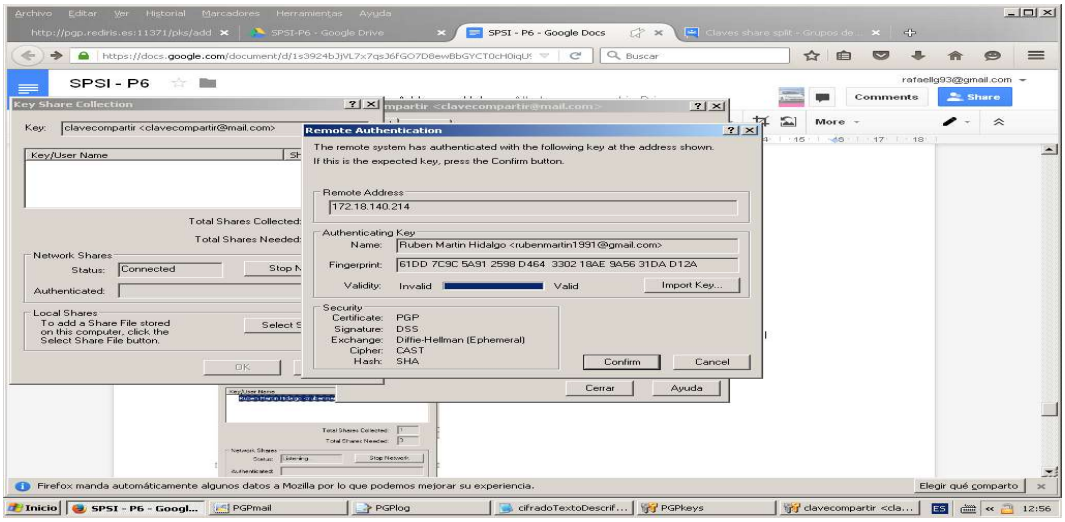
Ahora vamos obteniendo a través de la red las claves:



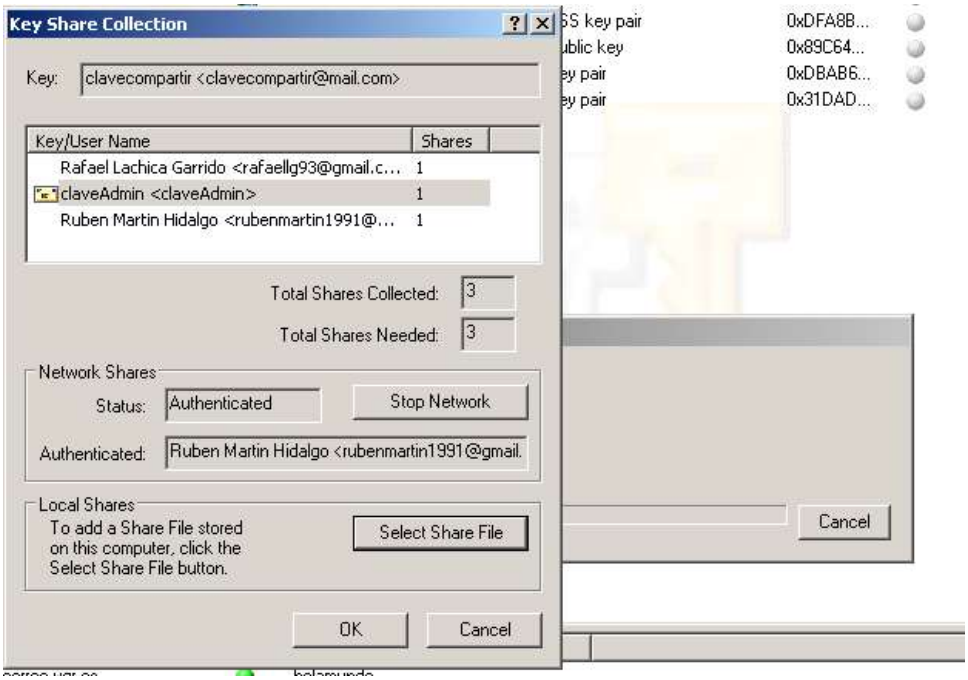
Y ya vamos obteniendo todas las claves, aquí vemos que ya hemos obtenido la del compañero:



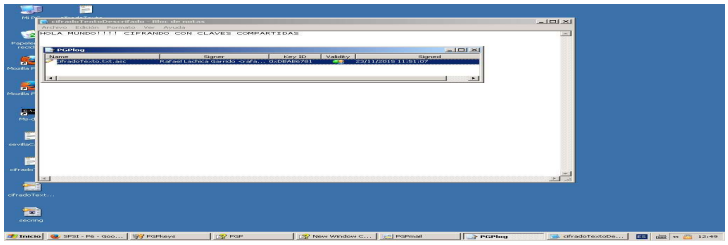
Cuando he recibido el fingerprint con el trozo de share key de mi compañero:



Juntamos todas las claves a través de la red, y le damos a OK, y obtenemos el mensaje descifrado. Para el usuario local claveAdmin lo obtenemos a través de select Share File:



Abrimos el mensaje descifrado:


HOLA RUBEN!!!! CIFRANDO CON CLAVES COMPARTIDAS
PGPfreeware