

Criptografía de clave pública: RSA

En <http://www-ma2.upc.es/~cripto/Q2.2015-16/> se encuentran los directorios RSA_RW y RSA_pseudo.

1. En RSA_pseudo hay una serie de ficheros del tipo *nombre.apellido_RSA_pseudo.enc* que es el resultado de cifrar un fichero con la clave pública RSA que se encuentra en el fichero *nombre.apellido_pubkeyRSA_pseudo.pem*. El cifrado se ha obtenido usando el comando:

```
openssl rsautl -encrypt -inkey nombre.apellido_pubkeyRSA_pseudo.pem -pubin -in nombre.apellido_pseudo.txt -out nombre.apellido_RSA_pseudo.enc
```

openssl está disponible en <https://www.openssl.org> aunque viene instalado por defecto en la mayoría de distribuciones linux, en la imágenes linux de la FIB lo está.

A partir del fichero *nombre.apellido_pubkeyRSA_pseudo.pem* hay que extraer la clave pública (*openssl* puede ayudar), factorizar el módulo (recomiendo usar *sage*, instalado en la imagen linux de la FIB, disponible para usarlo en la red <https://cloud.sagemath.com> o descargable en <http://www.sagemath.org>), calcular la clave privada, escribirla en un fichero en formato PEM para que pueda leerla *openssl* (para este paso puede ser útil el módulo *Crypto.PublicKey.RSA* de *python* pero se puede utilizar cualquier otra biblioteca) y por último descifrar, usando *openssl*, el fichero *nombre.apellido_RSA_pseudo.enc*.

2. En el directorio RSA_RW se encuentran los ficheros *nombre.apellido_pubkeyRSA_RW.pem* y *nombre.apellido_RSA_RW.enc*. Se tiene que hacer lo mismo pero para factorizar uno se puede inspirar en el artículo "Ron was wrong, Whit is right", <https://eprint.iacr.org/2012/064.pdf>.

Intercambiar información, por ejemplo usando el foro de prácticas, puede facilitar el trabajo.

Entrega

La entrega consistirá en cuatro ficheros, todos ellos empaquetados en un fichero zip o tar, dos con las claves privadas en formato PEM usadas para descifrar y los ficheros descifrados.

Os recuerdo que la entrega de las prácticas tendrá que hacerse a través del Racó, en un único fichero, y que para validar la entrega se ha de enviar un mensaje firmado digitalmente, y a poder ser cifrado, a fernando.martinez@upc.edu cuyo contenido ha de ser, como mínimo, el SHA512 del fichero entregado.