**PRÁCTICA 4**

Criptografía:

RSA 🡪 para que un algoritmo criptográfico sea seguro ha de ser público.

* Proteger la información
* Criptografía clásica
  + Clave simétrica o clave secreta 🡪 problema de distribución de la clave. Utiliza la misma clave para cifrar que para descifrar. Hay un problema con proteger la clave que descifra.

Un algoritmo al que le pasamos un texto en claro, se le aplica una clave de cifrado y obtenemos un criptograma. AES (Sistema de encriptación avanzado)

AES 256

AES 128

DES

A (m,K) = c A (c,K) = m

* + Clave asimétrica o clave pública. Una clave para cifrar y otra distinta para descifrar.

RSA (Visto en códigos, es en el problema de los primos y la factorización de los números primos)

A (m,K\_publica) = c A (c,K\_privada) = m

RSA 🡪 cifrar/ descifrar

Firma digital para la generación y verificación

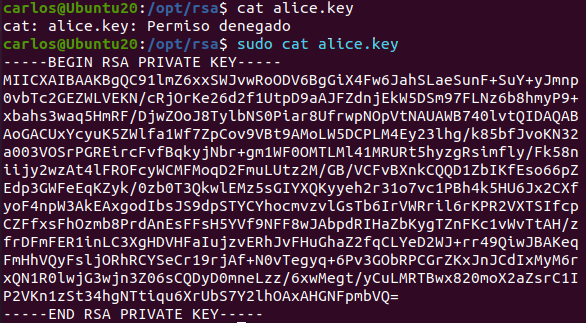
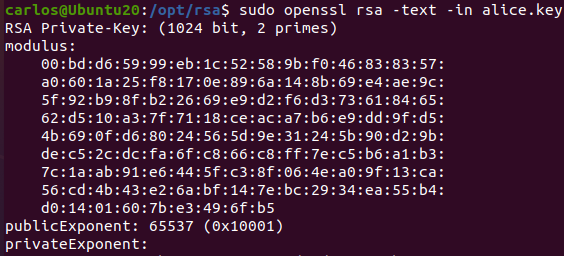
----------------------------

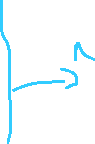
EJERCICIO 4 – COSAS VALEN PAL DOS

La clave privada ha de tenerla el servidor, porque como alguien consiga dicha clave privada, va a poder conocer todas las comunicaciones.

Una vez creado el directorio generamos la clave privada de RSA. Para la clave privada .key , y le tenemos que decir la longitud de la clave (longitud 2048 mirando el certificado, pero como es un ejemplo lo hacemos de 1024) lo ideal de normal es 2048 o 3056. Le hemos dicho a RSA que lo genere con esto tenemos (p,q,d) Texto

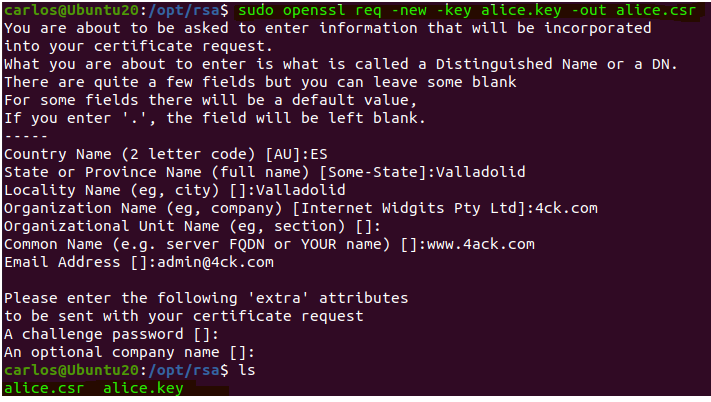
Descripción generada automáticamente



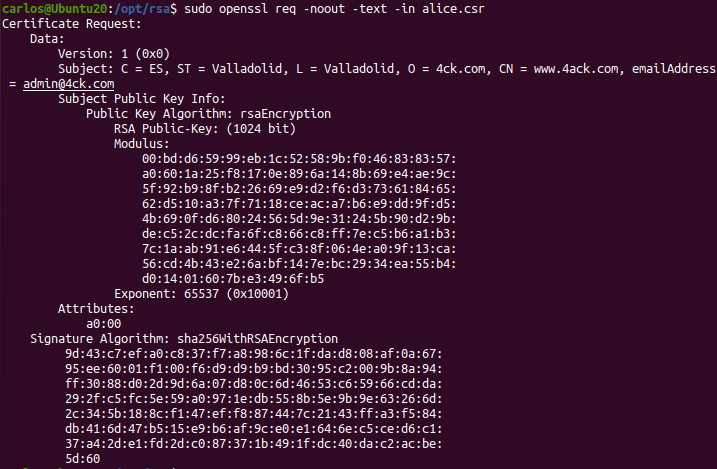


¿Por qué extension csr? 🡪

Nunca poner el correo tal cual en el certificado digital



Comando para ver que contiene esa solicitud de certificado:



Creación de un certificado digital auto firmado compatible con el estándar X.509:

Pantalla de un celular con letras

Descripción generada automáticamente con confianza media

Para el certificado la extensión es .crt

Movemos los ficheros a sus correspondientes directorios



Ahora con ls -l /etc/ssl, vemos que permisos tiene cada uno de los directorios, como vemos /private únicamente tiene permiso de lectura el root.

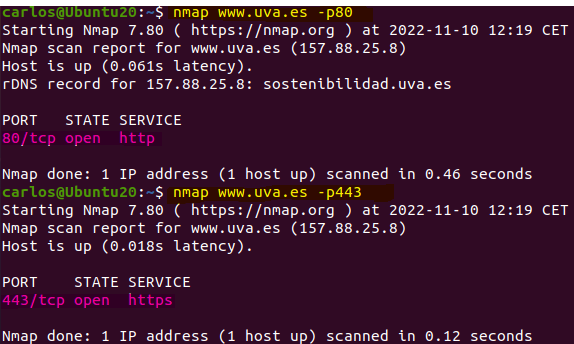
Texto

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

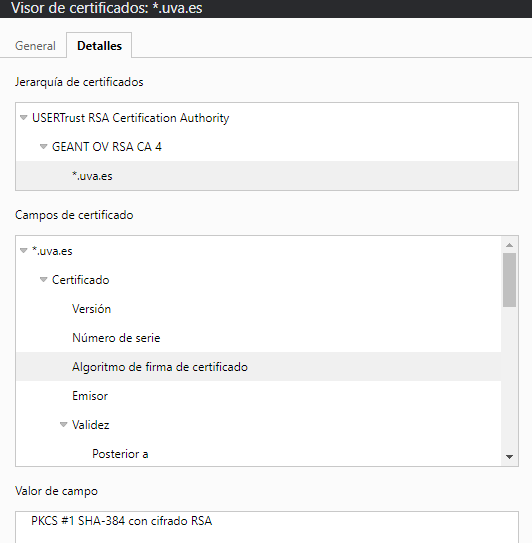
**Parte 2 (El sentido es hacer que la comunicación entre el cliente y el servidor vaya cifrada)**

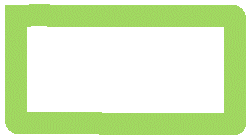


¿Para que sirve un certificado digital) El certificado digital (CIDAN) confidencialidad, integridad, autenticidad,disponibilidad, no repudio, también se podría meter una t de trazabilidad pero nah. (CERTIFICADO DIGITAL DE LA UVA)









La clave publica de RSA, permite cifrar. El cliente quiere la clave publica de RSA porque tiene que haber un intercambio seguro de claves

AES 256(M, K\_priv\_aes) = C

Enviar C



RSA(K\_priv\_RSA,() = K\_priv\_AES



Enviar C



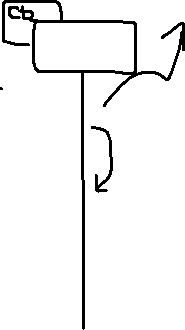
RSA(K\_pub\_RSA,K\_priv\_RSA) = C



Coge el aes-256 y genera una clave privada con aes. AES\_256 🡪 K\_priv\_AES



Certificado digital



302 es el código de respuesta http cuando se produce una redirección



Redireccion de HTTP a HTTPS (80🡪433)

Peticion HTTP (http://www.uva.es)



CLIENTE

WEB

Servidor web

Puerto 80 / TCP – HTTP

(no protege la información)

HTTPS 🡪 Si que proteg el puerto a HTTPS 443

SERVIDOR

