Práctica de OpenSSL

Instrucciones.

Para responder a cada una de las siguientes preguntas utilice **openssl.**

Preguntas.

1. ¿Cuál es el comando para obtener la versión de openssl?
2. ¿Para qué sirven los siguientes comandos? Explique a detalle
    a. Openssl speed blowfish
    b. Openssl speed md5
    c. Openssl speed sha
3. ¿Qué es lo que muestra el comando “prime”?
4. ¿Para qué sirve el comando “passwd”?
5. Suponga que se cuenta con un archivo **uaa.txt**
    a. ¿cómo realizaría el resumen del archivo a través de MD5?
    b. ¿cómo realizaría el resumen del archivo a través de SHA?
6. Generar una llave basada en el algoritmo AES simétrico de longitud 128. Almacenarla en un archivo llamado **llaveRSA.txt**.
7. Mediante el algoritmo DES encriptar un archivo llamado decimo.txt (poner texto en dicho archivo), especificar la contraseña: **uaa** y obtener un archivo de salida llamado: **octavoEncriptado.txt**.
    a. De ser posible, ¿cuál sería la forma de **desencriptar** y obtener el contenido del archivo **decimoEncriptado.txt**?
8. Generar una llave con el algoritmo asimétrico RSA de 1024 bits. Generar la llave en el archivo **iscRSA1024.key**
9. Especificar el comando con el cual firmaría digitalmente un archivo llamado **seguridad.txt** a través de una llave almacenada en el archivo **secreto.key**. Obtener un archivo con la firma digital en formato binario.
    a. ¿cómo realizaría la verificación del archivo firmado anteriormente?
10. Realice una llave pública (**public1.key**) a través de una llave privada (**private.key**) y utilice como contraseña: **1q2w3e$r**