SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

Grado en Ingeniería Informática

Universidad de Granada

Practica 3 Protocolos Criptográficos

16 de noviembre de 2018

Índice

En este documento se explica la tercera practica de la asignatura, que trata de aprender a utilizar la herramienta OpenSSL, y para completarla es necesrio entregar los 14 puntos de la misma, hay que entregar este pdf con los comandos y las capturas de pantalla necesarias para demostrar que se ha realizado la practica.
En esta ocasión trabajaremos con protocolos criptográficos, intentando entender su filosofía de trabajo.

This document explains the third practice of the subject, which tries to learn how to use the OpenSSL tool, and to complete it, it is necessary to deliver the 14 points of the same, this pdf must be delivered with the commands and screenshots necessary to demonstrate that the practice has been carried out.
This time we will work with cryptographic protocols, trying to understand their work philosophy.

Tareas a realizar

Hay que tener en cuenta que para la realización de esta practica simularemos que tenemos dos usuarios diferentes, por lo tanto habrá en ocasiones que generemos mas de un fichero de claves.

1. Generad un archivo sharedDSA.pem que contenga los parámetros. Mostrad los valores.

Para realizar esta tarea ejecutaremos en la consola el siguientes comando:

```
[usuario@portatil ~/] openssl dsaparam -text -outform PEM -out sharedDSA.pem 4096
Generating DSA parameters, 4096 bit long prime
This could take some time
...........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
.........+.............+........+.............+.+.....+..+...+...+........
..+.......++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
[usuario@portatil ~/] openssl dsaparam -text -noout -in sharedDSA.pem
    P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
  Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
  G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
```

```
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
```

2. Generad dos parejas de claves para los parámetros anteriores. La claves se almacenarán en los archivos <nombre>DSAkey.pem y <apellido>DSAkey.pem, No es necesario protegerlas por contraseña.

```
[usuario@portatil:~]$ openssl gendsa -out usuario1/DSAkey.pem sharedDSA.pem
Generating DSA key, 4096 bits
[usuario@portatil:~]$ openssl gendsa -out usuario2/DSAkey.pem sharedDSA.pem
Generating DSA key, 4096 bits
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario1/DSAkey.pem
read DSA key
Private-Key: (4096 bit)
  priv:
    66:e4:7d:73:3c:9f:94:1f:ea:0b:86:8d:ae:04:e2:
    e5:52:a4:dc:7d:f2:aa:59:cb:15:7c:02:54:67:07:
    0a:ac
  pub:
    75:f4:9f:4b:68:a3:25:52:c9:30:d9:67:1f:82:b3:
    f3:44:f8:16:5b:0f:8f:b8:70:94:84:ef:54:f8:5c:
    ce:a9:63:0f:43:5a:17:61:b3:1d:66:db:64:3f:ca:
    e5:b4:e1:96:b0:d5:3d:39:4f:b9:cc:16:90:8a:24:
    07:09:ed:32:d0:03:13:6c:a8:4a:09:47:44:eb:03:
    01:26:a9:00:58:57:39:23:8f:3e:e0:49:ff:c0:b9:
    fa:8d:a1:bc:36:9e:ec:28:e3:6d:ac:ef:3d:e8:d8:
    35:4e:a4:ff:82:cb:e3:87:cc:9f:44:f7:ae:c0:2b:
    66:85:0a:6e:8e:d1:a1:b3:83:a3:24:46:dd:3b:a9:
    49:f3:bd:cb:ac:29:2e:d6:18:4d:ea:f5:c9:a8:08:
    42:04:63:96:4c:d7:f4:38:09:a7:a1:6b:16:20:e5:
    e0:b4:7c:e8:1e:8d:61:35:10:65:31:c6:ed:ce:05:
    b3:a3:32:38:10:9f:c2:4e:8c:64:64:d9:39:c1:59:
    e9:53:5d:1c:d3:ff:9f:d8:69:24:30:a0:98:78:3c:
    3d:56:12:b9:f5:0e:e0:b5:81:43:4d:78:7b:ad:66:
    87:b7:77:c7:10:83:0e:a0:93:0b:c4:44:6b:8a:00:
    f8:5c:03:dd:20:de:00:1d:5d:6f:49:74:8d:f4:67:
    cc:ca:c3:89:cf:69:40:a3:b8:ab:ad:ba:6a:66:7b:
    27:42:ef:77:a8:fc:fa:20:ab:e0:ba:1e:2f:6e:40:
    49:9e:86:bc:90:be:4f:33:5d:c3:e2:47:1d:96:86:
    d6:5d:ab:e1:03:cb:5b:a1:5a:4c:91:b9:65:26:53:
    3f:ba:13:1c:f7:59:84:2b:7b:47:34:33:f6:09:62:
    75:57:ff:7b:f9:8c:e0:80:ee:13:18:1b:45:24:44:
    68:e5:80:f7:b3:99:cd:c4:ee:ad:cb:cf:74:2a:c5:
    81:9a:36:04:3c:3f:e4:a8:3a:e8:be:0c:07:b2:1a:
    b4:88:c0:e3:cf:74:00:93:5e:69:fd:68:f4:31:41:
    7a:1d:48:c5:70:d8:0a:e3:00:ec:64:43:98:a1:e3:
    7c:68:f0:64:4b:7d:11:fd:90:94:55:f9:95:56:4f:
```

```
    78:a3:59:eb:b2:e6:55:e1:57:2b:d9:d9:50:bf:bc:
    f8:86:de:ea:6c:73:06:70:d9:d3:0b:04:44:f8:89:
    e7:f7:e0:14:50:b4:d4:1c:7c:e1:fd:6a:7d:cd:d6:
    59:bb:f9:53:b4:f0:b8:2b:18:06:bd:c9:60:6c:a1:
    55:15:e6:fa:1a:86:80:72:12:a8:d6:c9:66:78:21:
    50:90:00:be:f5:7b:1c:ea:16:98:ab:7d:d4:58:73:
    3d:ed
P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
```

```
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSAkey.pem
read DSA key
Private-Key: (4096 bit)
  priv:
    27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
    16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
    d8:e7
  pub:
    17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
    cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
    f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
    a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
    be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
    bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
    8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
    6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
    c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
    89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
    12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
    fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
    5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
    b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
    40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
    6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
    35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
    da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
    e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
    7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
    ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
    60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
    3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
    0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
    7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
    30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
    99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:f0:b4:
    f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
    4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
    a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
    5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
    40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
    6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
    14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
    0e:d1
  P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
```

```
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
  Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
  G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
```

3. 'Extraed' la clave privada contenida en el archivo <nombre>DSAkey.pem a otro archivo que tenga por nombre <nombre>DSApriv.pem. Este archivo deberá estar protegido por contraseña. Mostrad sus valores. Haced lo mismo para el archivo <apellido>DSAkey.pem.

A continuación se muestran todos los comandos utilizados para realizar este apartado:

```
[usuario@portatil:~]$ openssl dsa -in usuario1/DSAkey.pem -outform PEM -out usuario1/
    DSApriv.pem
read DSA key
writing DSA key
[usuario@portatil:~]$ openssl dsa -aes-256-cbc -in usuario1/DSApriv.pem -out usuario1/
    DSApriv.pem.enc
```

```
read DSA key
writing DSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
[usuario@portatil:~]$ openssl dsa -in usuario2/DSAkey.pem -outform PEM -out usuario2/
    DSApriv.pem
read DSA key
writing DSA key
[usuario@portatil:~]$ openssl dsa -aes-256-cbc -in usuario2/DSApriv.pem -out usuario2/
    DSApriv.pem.enc
read DSA key
writing DSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario1/DSApriv.pem
read DSA key
Private-Key: (4096 bit)
  priv:
    66:e4:7d:73:3c:9f:94:1f:ea:0b:86:8d:ae:04:e2:
    e5:52:a4:dc:7d:f2:aa:59:cb:15:7c:02:54:67:07:
    0a:ac
  pub:
    75:f4:9f:4b:68:a3:25:52:c9:30:d9:67:1f:82:b3:
    f3:44:f8:16:5b:0f:8f:b8:70:94:84:ef:54:f8:5c:
    ce:a9:63:0f:43:5a:17:61:b3:1d:66:db:64:3f:ca:
    e5:b4:e1:96:b0:d5:3d:39:4f:b9:cc:16:90:8a:24:
    07:09:ed:32:d0:03:13:6c:a8:4a:09:47:44:eb:03:
    01:26:a9:00:58:57:39:23:8f:3e:e0:49:ff:c0:b9:
    fa:8d:a1:bc:36:9e:ec:28:e3:6d:ac:ef:3d:e8:d8:
    35:4e:a4:ff:82:cb:e3:87:cc:9f:44:f7:ae:c0:2b:
    66:85:0a:6e:8e:d1:a1:b3:83:a3:24:46:dd:3b:a9:
    49:f3:bd:cb:ac:29:2e:d6:18:4d:ea:f5:c9:a8:08:
    42:04:63:96:4c:d7:f4:38:09:a7:a1:6b:16:20:e5:
    e0:b4:7c:e8:1e:8d:61:35:10:65:31:c6:ed:ce:05:
    b3:a3:32:38:10:9f:c2:4e:8c:64:64:d9:39:c1:59:
    e9:53:5d:1c:d3:ff:9f:d8:69:24:30:a0:98:78:3c:
    3d:56:12:b9:f5:0e:e0:b5:81:43:4d:78:7b:ad:66:
    87:b7:77:c7:10:83:0e:a0:93:0b:c4:44:6b:8a:00:
    f8:5c:03:dd:20:de:00:1d:5d:6f:49:74:8d:f4:67:
    cc:ca:c3:89:cf:69:40:a3:b8:ab:ad:ba:6a:66:7b:
    27:42:ef:77:a8:fc:fa:20:ab:e0:ba:1e:2f:6e:40:
    49:9e:86:bc:90:be:4f:33:5d:c3:e2:47:1d:96:86:
    d6:5d:ab:e1:03:cb:5b:a1:5a:4c:91:b9:65:26:53:
    3f:ba:13:1c:f7:59:84:2b:7b:47:34:33:f6:09:62:
    75:57:ff:7b:f9:8c:e0:80:ee:13:18:1b:45:24:44:
    68:e5:80:f7:b3:99:cd:c4:ee:ad:cb:cf:74:2a:c5:
    81:9a:36:04:3c:3f:e4:a8:3a:e8:be:0c:07:b2:1a:
    b4:88:c0:e3:cf:74:00:93:5e:69:fd:68:f4:31:41:
    7a:1d:48:c5:70:d8:0a:e3:00:ec:64:43:98:a1:e3:
    7c:68:f0:64:4b:7d:11:fd:90:94:55:f9:95:56:4f:
    78:a3:59:eb:b2:e6:55:e1:57:2b:d9:d9:50:bf:bc:
    f8:86:de:ea:6c:73:06:70:d9:d3:0b:04:44:f8:89:
    e7:f7:e0:14:50:b4:d4:1c:7c:e1:fd:6a:7d:cd:d6:
    59:bb:f9:53:b4:f0:b8:2b:18:06:bd:c9:60:6c:a1:
    55:15:e6:fa:1a:86:80:72:12:a8:d6:c9:66:78:21:
    50:90:00:be:f5:7b:1c:ea:16:98:ab:7d:d4:58:73:
    3d:ed
  P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
```

```
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
  Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
  G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario1/DSApriv.pem.enc
read DSA key
Enter pass phrase for usuario1/DSApriv.pem.enc:
Private-Key: (4096 bit)
  priv:
    66:e4:7d:73:3c:9f:94:1f:ea:0b:86:8d:ae:04:e2:
    e5:52:a4:dc:7d:f2:aa:59:cb:15:7c:02:54:67:07:
    0a:ac
  pub:
    75:f4:9f:4b:68:a3:25:52:c9:30:d9:67:1f:82:b3:
    f3:44:f8:16:5b:0f:8f:b8:70:94:84:ef:54:f8:5c:
    ce:a9:63:0f:43:5a:17:61:b3:1d:66:db:64:3f:ca:
    e5:b4:e1:96:b0:d5:3d:39:4f:b9:cc:16:90:8a:24:
    07:09:ed:32:d0:03:13:6c:a8:4a:09:47:44:eb:03:
    01:26:a9:00:58:57:39:23:8f:3e:e0:49:ff:c0:b9:
    fa:8d:a1:bc:36:9e:ec:28:e3:6d:ac:ef:3d:e8:d8:
    35:4e:a4:ff:82:cb:e3:87:cc:9f:44:f7:ae:c0:2b:
```

```
    66:85:0a:6e:8e:d1:a1:b3:83:a3:24:46:dd:3b:a9:
    49:f3:bd:cb:ac:29:2e:d6:18:4d:ea:f5:c9:a8:08:
    42:04:63:96:4c:d7:f4:38:09:a7:a1:6b:16:20:e5:
    e0:b4:7c:e8:1e:8d:61:35:10:65:31:c6:ed:ce:05:
    b3:a3:32:38:10:9f:c2:4e:8c:64:64:d9:39:c1:59:
    e9:53:5d:1c:d3:ff:9f:d8:69:24:30:a0:98:78:3c:
    3d:56:12:b9:f5:0e:e0:b5:81:43:4d:78:7b:ad:66:
    87:b7:77:c7:10:83:0e:a0:93:0b:c4:44:6b:8a:00:
    f8:5c:03:dd:20:de:00:1d:5d:6f:49:74:8d:f4:67:
    cc:ca:c3:89:cf:69:40:a3:b8:ab:ad:ba:6a:66:7b:
    27:42:ef:77:a8:fc:fa:20:ab:e0:ba:1e:2f:6e:40:
    49:9e:86:bc:90:be:4f:33:5d:c3:e2:47:1d:96:86:
    d6:5d:ab:e1:03:cb:5b:a1:5a:4c:91:b9:65:26:53:
    3f:ba:13:1c:f7:59:84:2b:7b:47:34:33:f6:09:62:
    75:57:ff:7b:f9:8c:e0:80:ee:13:18:1b:45:24:44:
    68:e5:80:f7:b3:99:cd:c4:ee:ad:cb:cf:74:2a:c5:
    81:9a:36:04:3c:3f:e4:a8:3a:e8:be:0c:07:b2:1a:
    b4:88:c0:e3:cf:74:00:93:5e:69:fd:68:f4:31:41:
    7a:1d:48:c5:70:d8:0a:e3:00:ec:64:43:98:a1:e3:
    7c:68:f0:64:4b:7d:11:fd:90:94:55:f9:95:56:4f:
    78:a3:59:eb:b2:e6:55:e1:57:2b:d9:d9:50:bf:bc:
    f8:86:de:ea:6c:73:06:70:d9:d3:0b:04:44:f8:89:
    e7:f7:e0:14:50:b4:d4:1c:7c:e1:fd:6a:7d:cd:d6:
    59:bb:f9:53:b4:f0:b8:2b:18:06:bd:c9:60:6c:a1:
    55:15:e6:fa:1a:86:80:72:12:a8:d6:c9:66:78:21:
    50:90:00:be:f5:7b:1c:ea:16:98:ab:7d:d4:58:73:
    3d:ed
P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
```

```
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSApriv.pem
read DSA key
Private-Key: (4096 bit)
  priv:
    27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
    16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
    d8:e7
  pub:
    17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
    cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
    f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
    a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
    be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
    bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
    8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
    6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
    c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
    89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
    12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
    fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
    5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
    b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
    40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
    6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
    35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
    da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
    e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
    7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
    ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
    60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
    3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
    0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
    7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
    30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
    99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:f0:b4:
    f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
    4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
    a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
    5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
    40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
    6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
    14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
    0e:d1
  P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
```

```
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
  Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
  G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
[usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSApriv.pem.enc
read DSA key
Enter pass phrase for usuario2/DSApriv.pem.enc:
```

```
Private-Key: (4096 bit)
  priv:
    27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
    16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
    d8:e7
  pub:
    17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
    cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
    f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
    a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
    be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
    bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
    8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
    6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
    c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
    89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
    12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
    fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
    5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
    b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
    40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
    6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
    35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
    da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
    e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
    7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
    ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
    60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
    3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
    0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
    7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
    30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
    99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:f0:b4:
    f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
    4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
    a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
    5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
    40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
    6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
    14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
    0e:d1
  P:
    00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
    76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
    28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
    89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
    4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
    80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
    69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
    06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
    b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
    c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
    57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
    af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
    8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
    a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
    7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
    f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
    21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
    c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
    82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
    c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
    4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
    cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
    2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
    a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
    fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
    b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
    35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
    bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
    a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
    9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
    2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
    d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
    db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
```

```
    b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
    52:f5:e5
  Q:
    00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
    3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
    86:b5:11
    G:
    00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
    77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
    0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
    27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
    8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
    83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
    79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
    29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
    7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
    59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
    44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
    cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
    9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
    70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
    7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
    cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
    aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
    9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
    ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
    2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
    fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
    62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
    a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
    b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
    fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
    92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
    6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
    9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
    17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
    6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
    c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
    ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
    7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
    7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
    ec:c2:b1
```

4. Extraed en <nombre>DSApub.pem la clave pública contenida en el archivo <nombre>DSAkey.pem. De nuevo <nombre>DSApub.pem no debe estar cifrado ni protegido. Mostrad sus valores. Lo mismo para el archivo <apellido>DSAkey.pem.

```
[usuario@portatil:~]$ openssl dsa -pubout -outform PEM -in usuario1/DSAkey.pem -out
    usuario1/DSApub.pem
read DSA key
writing DSA key
[usuario@portatil:~]$
[usuario@portatil:~]$ openssl dsa -pubout -outform PEM -in usuario2/DSAkey.pem -out
    usuario2/DSApub.pem
read DSA key
writing DSA key
[usuario@portatil:~]$ openssl dsa -pubout -in usuario1/DSAkey.pem
-----BEGIN PUBLIC KEY-----
MIIGRjCCBDkGByqGSM44BAEwggQsAoICAQCdyt7tyYLi7GJ8m/dCsJkV9BZfxZV0
tm1z48AtZv3fFFxg/vRnF5MJSsaRFxRLUhEn1BgezTFVOEHYujj2EyBIBs3fvLMd
X/XDnRvxmh84NY7RDlNDmI2R+oG5rZxhHlIm0ynfX3YfoCFKSk6QhT1sRFEdvlHG
yk+098zM906CcrMEokY6s9cyaYiaMMoHKVpniRkBgWIF4NH8bAPG7KFFxJfXtL8L
mPjAHY6bmtsSmtSAQC6oeG9P8htOKdxnd7TQfpZt3u8lLRqBfQgzHqJmb/KPZfOC
1s1+PgRgUpUGnSr2ER3mfD4Lm5gWWQfwb7Sn1lIMI6BFz56ekll/xV0BUGfRgOL2
ysY7Z/FI3DGwnWbGNX26cL1tj4AytOCbkwu6ecJ6L6HAuY8II5k+3Ypdx4FepJ6f
```

```
YaSLmnsadXyZ2TQv3eDD70j9EtuqC4GZgUjGNKqcHzgyt+B8KyzzeeG9Bsx7uPcp
/B8asF1iafI02RzbaDUREFRzDf8IwoSxF3hmr41g9ubtkPQTGJoeO8RLGuIjRFP7
x9OyLsrq5TP62FNHvk8pNBLfycUKo5/nqCv9G/zNuuWFFU2TTIgHOyBdF3H6C+L7
gwNe+McSuCDHsgy1EiRAURFihIqw8eTcqix6/t7IPSpkC4GhlsRkhqvS8O21gcck
zUWkgpsLzIzJBwIhAPypEJTMxiN19zjGM81+zDBM2LVfkJDp4JYVQ5qle55DAoIC
ABwBBu9opARxzS4MN3JlgbqNv3ukO7nSOK2stqNJTUXizP5r4qnmv2qUsAH+1kNZ
hJcwRf1GqO6Fz761PgRfBzdh7q4M1DSXg12hc9Sffsu9A4Eiz8ZFMWHpwuYm+24g
uErXFDSBGkxFHCkyMYfzlgMkhooBSnFRmS93a+HpV8DkSst+5qkXAxPnIpi/seV4
F8Qx8jK34nibbLVrJwMbxE32BDy7KBFs66l5fz46PXsYEclBIB1zoypu/s95UK5h
egz+5z6VImad3wIJxrN0TUQ+Z5jq8ZboN6qcTqjZgDwz4AnXUHGZDoWJ1X6zk+kw
1rUW00aWfvBUX2mvaOOe143mD7a6AMigQJsOjj26pO5g/wI2JB42dEZIzJXHrW3S
MHEOIMHlkEfXpmwefCOinbqgPij07eUsZfndYF6KSXJhUZdGB7kt8chHEWIZS13F
baovx1aXugFcuatHtxdMSF9+cesyoxWXzz4J2YzUuBAsy/08jCnJjxCuP6Uu52Fs
bnomcTS73+STRZQMxvQT8+Z+9Iw2mr9BNyhhM1wbmDT/7wPo3GcVntLLTmIbF6GY
iYy5yw23f6JxqH4HWjTJONXua5dCr4WuEejG8Rc/rh2m5SCJixv20JP2KQ2OsNJL
USwJrvCPQevGB1d9t0uenc7f+Th4x6aKSpGHBoOfDA9OA4ICBQACggIARA9MWn0y
+RMlxKOiSYpg1mZjCh9dqg+zuFga3FvB8e85KBlg5kQIM8kmmTAKUqjZ5yhGRyla
13lvYplmB6hrw3DU9UfjQyXnhLHZCexZjIBAOilAXJPumJ6wN/xOkj7ElN4W1NbL
TOf/sbEc/pH8xjHlRdW/ZmiFOm8xIYE2bB5tSPtj9sp/vShRkiI7upYJijuHNX9L
Aqavg6zdq98BAmidGwAsBxjdWUqLgHasWyRFO9FRhIUwF34iFpd5Bw0fvbhekQ3k
oAp1amxrAEySI9TIVTirAi1Fg4Z+L4A6RnVNgi4R1G8WMKzVNcbHhjnxmYLxFkq7
7ht8CihwErVSxRomxdkkh2p3LZZ+OwfbAQaCxuyrFi6DvSJYsSXwWXAmQ/vsknYl
WGuMmMO/z7USbKqdOJeI4x2wzG/u4YHOqm6OijPgMw1xobv/vKIuVQCQ5HGe+irk
iq9nmdHPjiL1kJWvP34/4V9qz5PYR22UOVPgLi8Y8KKBhpmwAzciNo5OMFgd891Q
l4iKylHsqIxeSIbBbskxzJsZOMXus5mTbH8KdU2VkojosV2ui9F0savhpTAaDT4/
HF6UWCb4cKGm/KPvHIFOmGnVix6U6tWBWKiwbJEQ/7/2qTwQ/n70+dZS0k3IV4A3
R6UGJd2u8zXy5dsSEEESE5SZCQ78CtGeouY=
-----END PUBLIC KEY-----
[usuario@portatil:~]$ openssl dsa -pubout -in usuario2/DSAkey.pem
-----BEGIN PUBLIC KEY-----
MIIGRjCCBDkGByqGSM44BAEwggQsAoICAQCdyt7tyYLi7GJ8m/dCsJkV9BZfxZV0
tm1z48AtZv3fFFxg/vRnF5MJSsaRFxRLUhEn1BgezTFVOEHYujj2EyBIBs3fvLMd
X/XDnRvxmh84NY7RDlNDmI2R+oG5rZxhHlIm0ynfX3YfoCFKSk6QhT1sRFEdvlHG
yk+098zM906CcrMEokY6s9cyaYiaMMoHKVpniRkBgWIF4NH8bAPG7KFFxJfXtL8L
mPjAHY6bmtsSmtSAQC6oeG9P8htOKdxnd7TQfpZt3u8lLRqBfQgzHqJmb/KPZfOC
1s1+PgRgUpUGnSr2ER3mfD4Lm5gWWQfwb7Sn1lIMI6BFz56ekll/xV0BUGfRgOL2
ysY7Z/FI3DGwnWbGNX26cL1tj4AytOCbkwu6ecJ6L6HAuY8II5k+3Ypdx4FepJ6f
YaSLmnsadXyZ2TQv3eDD70j9EtuqC4GZgUjGNKqcHzgyt+B8KyzzeeG9Bsx7uPcp
/B8asF1iafI02RzbaDUREFRzDf8IwoSxF3hmr41g9ubtkPQTGJoeO8RLGuIjRFP7
x9OyLsrq5TP62FNHvk8pNBLfycUKo5/nqCv9G/zNuuWFFU2TTIgHOyBdF3H6C+L7
gwNe+McSuCDHsgy1EiRAURFihIqw8eTcqix6/t7IPSpkC4GhlsRkhqvS8O21gcck
zUWkgpsLzIzJBwIhAPypEJTMxiN19zjGM81+zDBM2LVfkJDp4JYVQ5qle55DAoIC
ABwBBu9opARxzS4MN3JlgbqNv3ukO7nSOK2stqNJTUXizP5r4qnmv2qUsAH+1kNZ
hJcwRf1GqO6Fz761PgRfBzdh7q4M1DSXg12hc9Sffsu9A4Eiz8ZFMWHpwuYm+24g
uErXFDSBGkxFHCkyMYfzlgMkhooBSnFRmS93a+HpV8DkSst+5qkXAxPnIpi/seV4
F8Qx8jK34nibbLVrJwMbxE32BDy7KBFs66l5fz46PXsYEclBIB1zoypu/s95UK5h
egz+5z6VImad3wIJxrN0TUQ+Z5jq8ZboN6qcTqjZgDwz4AnXUHGZDoWJ1X6zk+kw
1rUW00aWfvBUX2mvaOOe143mD7a6AMigQJsOjj26pO5g/wI2JB42dEZIzJXHrW3S
MHEOIMHlkEfXpmwefCOinbqgPij07eUsZfndYF6KSXJhUZdGB7kt8chHEWIZS13F
baovx1aXugFcuatHtxdMSF9+cesyoxWXzz4J2YzUuBAsy/08jCnJjxCuP6Uu52Fs
bnomcTS73+STRZQMxvQT8+Z+9Iw2mr9BNyhhM1wbmDT/7wPo3GcVntLLTmIbF6GY
iYy5yw23f6JxqH4HWjTJONXua5dCr4WuEejG8Rc/rh2m5SCJixv20JP2KQ2OsNJL
USwJrvCPQevGB1d9t0uenc7f+Th4x6aKSpGHBoOfDA9OA4ICBQACggIABKiaBJgz
GWnYhiNMyoAv3h7GHmxr2MnoS2ju+lg4Q5nYTQQa5teQ7Im1NoKeHCIG/NL3xtcN
zzQxnS8FQYET1mGE9rRQuZ4uhyEUWjG4aHLpJNn8pzorZjfs+wq8SgsHFz37dvNG
5krhra6CLBp/MMKIdbYdx7eNceZ45IXyZDRx6GKbBWD9wLS+C7lObVG83hyyjIHf
baOMtlNvKz0B2mH9HwP+sxnZ8Imrtj+vd+ihl7WT+8U5T9mnAnVcGmJ2+pvq6aFY
qgzWVF2MFSZTROtfCuSaskgTxPd3V90x/Ct4lav5FdOoG2NMOxTGzXK0XWezGxzB
ebHYw3JVq9b/HLOZc83F1rVEIJA1sl0hlXbMTDdm70f9WgXM9w21d1GJ9P3c3q0+
fwCEhM50rofL3LG4szbM8DxPlCVw/A0ll/lnTH+1mE15nK6LKGOvm+TNhbNVL6ts
wfd1QHENOViY3aaIUQtvbHXpVSCalX0wZk3VE2qCTuO5gFv+zh9zpuAe4nDVqeC5
2bOu4Ev9Z40m/HSNQhhqVyG+95mucj/xpfaIKS8CyZ/FaB4jcDkNFmfgS+KtgFTb
83b2pcdnJVmdnfatZUxDRamekRCcZ6zQZcdhwglIPAtIhIbalT61h8uXzSpMNECE
7ogh5Js4nHqkQ2xaO7AzHsaMxsw3etduXXA=
-----END PUBLIC KEY-----
```

5. Coged un archivo cualquiera cualquiera, que actuará como entrada, con al menos 128 bytes. En adelante me referiré a él como *message*, pero podéis llamarlo como os parezca.

```
[usuario@portatil:~]$ dd bs=128 count=1 </dev/urandom > /tmp/message
1+0 registros leídos
1+0 registros escritos
128 bytes copied, 0,00019602 s, 653 kB/s
[usuario@portatil:~]$ hexdump usuario1/message
0000000 8886 8ea6 ed2a 67d7 0226 10a8 bc18 8ac6
0000010 e85a 7f09 70a4 d8a6 a490 d5c9 f01a 36a1
0000020 4a1a 4817 3aff 5899 b4a8 dd8c c207 5347
0000030 1995 2dc8 42ea f9d5 d2c0 081c fcf0 fc35
0000040 57c2 95cc 38f7 feb8 4bdf 004d 8fab cda1
0000050 7069 67e0 dc09 285b f6bb 7a97 6983 1339
0000060 159d 89ad 345e 9904 fce3 4a9d 639f 4a71
0000070 c59b 767a 016f e36f b7e6 0556 0d7b b1e2
0000080
```

6. Firmad directamente el archivo message empleando el comando openssl pkeyutl sin calcular valores hash, la firma deberá almacenarse en un archivo llamado, por ejemplo, message.sign. Mostrad el archivo con la firma.

```
[usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario1/DSAkey.pem -in /tmp/message -
    out /tmp/message.sign
[usuario@portatil:~]$ hexdump /tmp/message.sign
0000000 4530 2002 e70b 6ea7 dc3f 0776 53a1 7fa4
0000010 8546 5c49 2e2c 1a5d 56d3 3d7a 7463 d537
0000020 0477 5e5c 2102 da00 875d 6822 b3d8 1530
0000030 3376 7882 a13d 6227 6e23 f5a9 ffac 940d
0000040 7335 63de e3e6 00fd
0000047
[usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario2/DSAkey.pem -in /tmp/message -
    out /tmp/message.sign
[usuario@portatil:~]$ hexdump /tmp/message.sign
0000000 4530 2002 e15a 1702 283f dccf bb78 36dd
0000010 1d81 d630 37dc 5113 4159 b719 0b0e 7cd0
0000020 9c1a f1d4 2102 8400 ac17 f17e d59b 4777
0000030 dbc7 8a62 6892 3eff 68cc 30d4 0c15 7aa4
0000040 f834 5566 35e3 0031
0000047
```

7. Construid un archivo message2 diferente de message tal que la verificación de la firma message.sign sea correcta con respecto al archivo message2.

Como el comando pkeyutl trunca, la comprobación podemos realizar los siguientes comandos para comprobar este echo.

```
[usuario@portatil:~]$ dd bs=32 count=1 </dev/urandom > /tmp/extra
1+0 registros leídos
1+0 registros escritos
32 bytes copied, 2,5534e-05 s, 1,3 MB/s
[usuario@portatil:~]$ cat /tmp/message > /tmp/message2
[usuario@portatil:~]$ cat /tmp/extra >> /tmp/message2
[usuario@portatil:~]$ hexdump /tmp/message
0000000 21b1 276b 8b08 1d98 73a4 653a f2e4 a87b
```

```
0000010 903b 196d 52e6 7441 d11a 4a76 fcbd 98c5
0000020 d178 582b 1456 af12 63de e8ef 7af5 e61f
0000030 cd33 2252 6ba6 f11a 46f9 55c8 a7f6 1931
0000040 150d c9f5 be05 501d a3cf 9747 c894 2eff
0000050 5bf3 f327 bc8b 33fe 48c1 d3d8 bae3 b879
0000060 ce82 a841 d7bd c668 a7b7 7135 d513 b4d7
0000070 3358 ec34 4485 8d1f 5d56 77e2 e45b 6540
0000080
[usuario@portatil:~]$ hexdump /tmp/message2
0000000 21b1 276b 8b08 1d98 73a4 653a f2e4 a87b
0000010 903b 196d 52e6 7441 d11a 4a76 fcbd 98c5
0000020 d178 582b 1456 af12 63de e8ef 7af5 e61f
0000030 cd33 2252 6ba6 f11a 46f9 55c8 a7f6 1931
0000040 150d c9f5 be05 501d a3cf 9747 c894 2eff
0000050 5bf3 f327 bc8b 33fe 48c1 d3d8 bae3 b879
0000060 ce82 a841 d7bd c668 a7b7 7135 d513 b4d7
0000070 3358 ec34 4485 8d1f 5d56 77e2 e45b 6540
0000080 eb85 7f8b 6c2a 5a79 4b1d 9b77 a479 254d
0000090 1f28 1513 e9c3 bb50 de94 44c3 4b07 b78b
00000a0
[usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario1/DSAkey.pem -in /tmp/message -
    out /tmp/message.sign
[usuario@portatil:~]$ openssl pkeyutl -verify -inkey usuario1/DSAkey.pem -sigfile /tmp/
    message.sign -in /tmp/message
Signature Verified Successfully
[usuario@portatil:~]$ openssl pkeyutl -verify -inkey usuario1/DSAkey.pem -sigfile /tmp/
    message.sign -in /tmp/message2
Signature Verified Successfully
```

8. Calculad el valor hash del archivo con la clave pública nombreDSApub.pem usando sha384 con salida hexadecinal con bloques de dos caracteres separados por dos puntos. Mostrad los valores por salida estándar y guardadlo en nombreDSApub.sha384.

```
[usuario@portatil:~]$ openssl dgst -sha384 -c -out usuario1/DSApub.pem.sha384 usuario1/
    DSApub.pem
[usuario@portatil:~]$ cat usuario1/DSApub.pem.sha384
SHA384(usuario1/DSApub.pem)= 19:39:61:3a:6e:75:fe:24:02:a5:1b:09:1e:0a:44:4a:5e:9c:4c
    :68:87:fa:e0:c2:a4:84:b6:23:b9:94:98:97:df:7a:77:6e:eb:13:bd:70:73:8e:0a:d9:70:f4
    :02:94
```

9. Calculad el valor hash de message2 usando una función hash de 160 bits[1] con salida binaria. Guardad el hash en message2.<algoritmo>y mostrad su contenido.

```
[usuario@portatil:~]$ openssl dgst -c -binary -sha1 -out /tmp/message2.sha1 /tmp/message2
[usuario@portatil:~]$ hexdump /tmp/message2.sha1
0000000 2b5e cd96 71c2 d8cb 33c2 18c1 f61c 030a
0000010 0c5a 1efa
0000014
[usuario@portatil:~]$ ls -la /tmp/message2.sha1
-rw-rw-r-- 1 usuario usuario 20 nov  5 22:10 /tmp/message2.sha1
```

Hay que tener en cuenta que el fichero de hash en binario solo tiene un tamaño de 20 bytes, ya que 160 bits dividido entre 8 son igual a 20 bytes.

10. Firmad el archivo message2 mediante el comando openssl dgst y la función hash del punto anterior. La firma deberá almacenarse en un archivo llamado, por ejemplo, message2.sign.

```
[usuario@portatil:~]$
```

11. Verificad la firma message2.sign con los archivos message y message2 empleando el comando openssl dgst.

```
[usuario@portatil:~]$
```

12. Verificad que message2.sign es una firma correcta para message2 pero empleando el comando openssl pkeyutl

```
[usuario@portatil:~]$
```

13. Generad el valor HMAC del archivo sharedDSA.pem con clave '12345' mostrándolo por pantalla.

```
[usuario@portatil:~]$
```

14. Simulad una ejecución completa del protocolo Estación a Estación. Para ello emplearemos como claves para firma/verificación las generadas en esta práctica, y para el protocolo DH emplearemos las claves asociadas a curvas elípticas de la práctica anterior junto con las de otro usuario simulado que deberéis generar nuevamente.

Por ejemplo, (y teniendo en cuenta que el algoritmo simétrico a utilizar en el protocolo estación a estación será AES-128 en modo CFB8.) si mi clave privada está en javierECpriv.pem y la clave pública del otro usuario está en lobilloECpub.pem, el comando para generar la clave derivada será:

```
[usuario@portatil:~]$ openssl pkeyutl -derive -inkey javierECpriv.pem -peerkey
    lobilloECpub.pem -out key.bin
```

```
[usuario@portatil:~]$
```

Referencias

[1] Openssl, cryptography and ssl/tls toolkit, Consultado el 16 de noviembre de 2018. https://www.openssl.org/docs/man1.0.2/apps/openssl-dgst.html.