

Practica 3 Protocolos Criptográficos

16 de noviembre de 2018

Índice

1	Generad un archivo sharedDSA.pem que contenga los parámetros. Mostrad los valores.	1
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.	2
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.	5
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.	12
5	Coged un archivo cualquiera cualquiera, que actuará como entrada, con al menos 128 bytes. En adelante me referiré a él como <i>message</i> , pero podéis llamarlo como os parezca.	14
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.	14
7	Construid un archivo message2 diferente de message tal que la verificación de la firma message.sign sea correcta con respecto al archivo message2.	14
8	Calculad el valor hash del archivo con la clave pública nombreDSAPub.pem usando sha384 con salida hexadecimal con bloques de dos caracteres separados por dos puntos. Mostrad los valores por salida estándar y guardadlo en nombreDSAPub.sha384.	15
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.	15
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.	16
11	Verificad la firma message2.sign con los archivos message y message2 empleando el comando openssl dgst.	16
12	Verificad que message2.sign es una firma correcta para message2 pero empleando el comando openssl pkeyutl	16
13	Generad el valor HMAC del archivo sharedDSA.pem con clave '12345' mostrándolo por pantalla.	16
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.	16

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.


```

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

```

1 [usuario@portatil:~]$ openssl gendrsa -out usuario1/Dsakey.pem sharedDsa.pem
2 Generating DSA key, 4096 bits
3 [usuario@portatil:~]$ openssl gendrsa -out usuario2/Dsakey.pem sharedDsa.pem
4 Generating DSA key, 4096 bits
5 [usuario@portatil:~]$ openssl dsa -text -noout -in usuario1/Dsakey.pem
6 read DSA key
7 Private-Key: (4096 bit)
8   priv:
9     66:e4:7d:73:3c:9f:94:1f:ea:0b:86:8d:ae:04:e2:
10    e5:52:a4:dc:7d:f2:aa:59:cb:15:7c:02:54:67:07:
11    0a:ac
12   pub:
13    75:f4:9f:4b:68:a3:25:52:c9:30:d9:67:1f:82:b3:
14    f3:44:f8:16:5b:0f:8f:b8:70:94:84:ef:54:f8:5c:
15    ce:a9:63:0f:43:5a:17:61:b3:1d:66:db:64:3f:ca:
16    e5:b4:e1:96:b0:d5:3d:39:4f:b9:cc:16:90:8a:24:
17    07:09:ed:32:d0:03:13:6c:a8:4a:09:47:44:eb:03:
18    01:26:a9:00:58:57:39:23:8f:3e:e0:49:ff:c0:b9:
19    fa:8d:a1:bc:36:9e:ec:28:e3:6d:ac:ef:3d:e8:d8:
20    35:4e:a4:ff:82:cb:e3:87:cc:9f:44:f7:ae:c0:2b:
21    66:85:0a:6e:8e:d1:a1:b3:83:a3:24:46:dd:3b:a9:
22    49:f3:bd:cb:ac:29:2e:d6:18:4d:ea:f5:c9:a8:08:
23    42:04:63:96:4c:d7:f4:38:09:a7:a1:6b:16:20:e5:
24    e0:b4:7c:e8:1e:8d:61:35:10:65:31:c6:ed:ce:05:
25    b3:a3:32:38:10:9f:c2:4e:8c:64:64:d9:39:c1:59:
26    e9:53:5d:1c:d3:ff:9f:d8:69:24:30:a0:98:78:3c:
27    3d:56:12:b9:f5:0e:e0:b5:81:43:4d:78:7b:ad:66:
28    87:b7:77:c7:10:83:0e:a0:93:0b:c4:44:6b:8a:00:
29    f8:5c:03:dd:20:de:00:1d:5d:6f:49:74:8d:f4:67:
30    cc:ca:c3:89:cf:69:40:a3:b8:ab:ad:ba:6a:66:7b:
31    27:42:ef:77:a8:fc:fa:20:ab:e0:ba:1e:2f:6e:40:
32    49:9e:86:bc:90:be:4f:33:5d:c3:e2:47:1d:96:86:
33    d6:5d:ab:e1:03:cb:5b:a1:5a:4c:91:b9:65:26:53:
34    3f:ba:13:1c:f7:59:84:2b:7b:47:34:33:f6:09:62:
35    75:57:ff:7b:f9:8c:e0:80:ee:13:18:1b:45:24:44:
36    68:e5:80:f7:b3:99:cd:c4:ee:ad:cb:cf:74:2a:c5:
37    81:9a:36:04:3c:3f:e4:a8:3a:e8:be:0c:07:b2:1a:
38    b4:88:c0:e3:cf:74:00:93:5e:69:fd:68:f4:31:41:
39    7a:1d:48:c5:70:d8:0a:e3:00:ec:64:43:98:a1:e3:
40    7c:68:f0:64:4b:7d:11:fd:90:94:55:f9:95:56:4f:

```

```

41 78:a3:59:eb:b2:e6:55:e1:57:2b:d9:d9:50:bf:bc:
42 f8:86:de:ea:6c:73:06:70:d9:d3:0b:04:44:f8:89:
43 e7:f7:e0:14:50:b4:d4:1c:7c:e1:fd:6a:7d:cd:d6:
44 59:bb:f9:53:b4:f0:b8:2b:18:06:bd:c9:60:6c:a1:
45 55:15:e6:fa:1a:86:80:72:12:a8:d6:c9:66:78:21:
46 50:90:00:be:f5:7b:1c:ea:16:98:ab:7d:d4:58:73:
47 3d:ed
48 P:
49 00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
50 76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
51 28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
52 89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
53 4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
54 80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
55 69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
56 06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
57 b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
58 c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
59 57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
60 af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
61 8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
62 a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
63 7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
64 f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
65 21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
66 c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
67 82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
68 c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
69 4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
70 cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
71 2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
72 a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
73 fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
74 b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
75 35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
76 bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
77 a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
78 9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
79 2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
80 d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
81 db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
82 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
83 52:f5:e5
84 Q:
85 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
86 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
87 86:b5:11
88 G:
89 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
90 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
91 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
92 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
93 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
94 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
95 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
96 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
97 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
98 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
99 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
100 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
101 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
102 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
103 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
104 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
105 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
106 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
107 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:0d:26:
108 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
109 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
110 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
111 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
112 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
113 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
114 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
115 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:

```

```
116 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
117 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
118 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
119 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
120 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
121 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
122 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
123 ec:c2:b1
124 [usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSAkey.pem
125 read DSA key
126 Private-Key: (4096 bit)
127   priv:
128     27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
129     16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
130     d8:e7
131   pub:
132     17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
133     cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
134     f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
135     a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
136     be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
137     bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
138     8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
139     6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
140     c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
141     89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
142     12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
143     fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
144     5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
145     b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
146     40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
147     6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
148     35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
149     da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
150     e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
151     7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
152     ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
153     60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
154     3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
155     0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
156     7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
157     30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
158     99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:0f:b4:
159     f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
160     4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
161     a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
162     5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
163     40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
164     6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
165     14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
166     0e:d1
167   P:
168     00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
169     76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
170     28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
171     89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
172     4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
173     80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
174     69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
175     06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
176     b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
177     c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
178     57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
179     af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
180     8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
181     a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
182     7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
183     f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
184     21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
185     c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
186     82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
187     c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
188     4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
189     cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
190     2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
```

```

191 a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
192 fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
193 b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
194 35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
195 bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
196 a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
197 9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
198 2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
199 d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
200 db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
201 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
202 52:f5:e5
203 Q:
204 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
205 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
206 86:b5:11
207 G:
208 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
209 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
210 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
211 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
212 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
213 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
214 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
215 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
216 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
217 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
218 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
219 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
220 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
221 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
222 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
223 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
224 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
225 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
226 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
227 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
228 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
229 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
230 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
231 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
232 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
233 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
234 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
235 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
236 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
237 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
238 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
239 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
240 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
241 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
242 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:

```

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

```



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

```
78 c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
79 82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
80 c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
81 4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
82 cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
83 2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
84 a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
85 fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
86 b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
87 35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
88 bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
89 a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
90 9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
91 2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
92 d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
93 db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
94 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
95 52:f5:e5
96 Q:
97 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
98 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
99 86:b5:11
100 G:
101 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
102 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
103 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
104 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
105 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
106 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
107 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
108 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
109 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
110 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
111 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
112 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
113 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
114 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
115 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
116 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
117 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
118 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
119 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
120 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
121 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
122 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
123 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
124 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
125 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
126 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
127 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
128 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
129 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
130 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
131 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
132 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
133 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
134 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
135 ec:c2:b1
136 [usuario@portatil:~]$ openssl dsa -text -noout -in usuario1/DSApriv.pem.enc
137 read DSA key
138 Enter pass phrase for usuario1/DSApriv.pem.enc:
139 Private-Key: (4096 bit)
140   priv:
141     66:e4:7d:73:3c:9f:94:1f:ea:0b:86:8d:ae:04:e2:
142     e5:52:a4:dc:7d:f2:aa:59:cb:15:7c:02:54:67:07:
143     0a:ac
144   pub:
145     75:f4:9f:4b:68:a3:25:52:c9:30:d9:67:1f:82:b3:
146     f3:44:f8:16:5b:0f:8f:b8:70:94:84:ef:54:f8:5c:
147     ce:a9:63:0f:43:5a:17:61:b3:1d:66:db:64:3f:ca:
148     e5:b4:e1:96:b0:d5:3d:39:4f:b9:cc:16:90:8a:24:
149     07:09:ed:32:d0:03:13:6c:a8:4a:09:47:44:eb:03:
150     01:26:a9:00:58:57:39:23:8f:3e:e0:49:ff:c0:b9:
151     fa:8d:a1:bc:36:9e:ec:28:e3:6d:ac:ef:3d:e8:d8:
152     35:4e:a4:ff:82:cb:e3:87:cc:9f:44:f7:ae:c0:2b:
```

```

153 66:85:0a:6e:8e:d1:a1:b3:83:a3:24:46:dd:3b:a9:
154 49:f3:bd:cb:ac:29:2e:d6:18:4d:ea:f5:c9:a8:08:
155 42:04:63:96:4c:d7:f4:38:09:a7:a1:6b:16:20:e5:
156 e0:b4:7c:e8:1e:8d:61:35:10:65:31:c6:ed:ce:05:
157 b3:a3:32:38:10:9f:c2:4e:8c:64:64:d9:39:c1:59:
158 e9:53:5d:1c:d3:ff:9f:d8:69:24:30:a0:98:78:3c:
159 3d:56:12:b9:f5:0e:e0:b5:81:43:4d:78:7b:ad:66:
160 87:b7:77:c7:10:83:0e:a0:93:0b:c4:44:6b:8a:00:
161 f8:5c:03:dd:20:de:00:1d:5d:6f:49:74:8d:f4:67:
162 cc:ca:c3:89:cf:69:40:a3:b8:ab:ad:ba:6a:66:7b:
163 27:42:ef:77:a8:fc:fa:20:ab:e0:ba:1e:2f:6e:40:
164 49:9e:86:bc:90:be:4f:33:5d:c3:e2:47:1d:96:86:
165 d6:5d:ab:e1:03:cb:5b:a1:5a:4c:91:b9:65:26:53:
166 3f:ba:13:1c:f7:59:84:2b:7b:47:34:33:f6:09:62:
167 75:57:ff:7b:f9:8c:e0:80:ee:13:18:1b:45:24:44:
168 68:e5:80:f7:b3:99:cd:c4:ee:ad:cb:cf:74:2a:c5:
169 81:9a:36:04:3c:3f:e4:a8:3a:e8:be:0c:07:b2:1a:
170 b4:88:c0:e3:cf:74:00:93:5e:69:fd:68:f4:31:41:
171 7a:1d:48:c5:70:d8:0a:e3:00:ec:64:43:98:a1:e3:
172 7c:68:f0:64:4b:7d:11:fd:90:94:55:f9:95:56:4f:
173 78:a3:59:eb:b2:e6:55:e1:57:2b:d9:d9:50:bf:bc:
174 f8:86:de:ea:6c:73:06:70:d9:d3:0b:04:44:f8:89:
175 e7:f7:e0:14:50:b4:d4:1c:7c:e1:fd:6a:7d:cd:d6:
176 59:bb:f9:53:b4:f0:b8:2b:18:06:bd:c9:60:6c:a1:
177 55:15:e6:fa:1a:86:80:72:12:a8:d6:c9:66:78:21:
178 50:90:00:be:f5:7b:1c:ea:16:98:ab:7d:d4:58:73:
179 3d:ed
180 P:
181 00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
182 76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
183 28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
184 89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
185 4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
186 80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
187 69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
188 06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
189 b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
190 c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
191 57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
192 af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
193 8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
194 a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
195 7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
196 f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
197 21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
198 c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
199 82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
200 c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
201 4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
202 cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
203 2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
204 a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
205 fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
206 b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
207 35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
208 bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
209 a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
210 9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
211 2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
212 d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
213 db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
214 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
215 52:f5:e5
216 Q:
217 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
218 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
219 86:b5:11
220 G:
221 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
222 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
223 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
224 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
225 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
226 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
227 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:

```

```
228 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
229 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
230 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
231 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
232 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
233 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
234 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
235 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
236 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
237 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
238 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
239 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
240 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
241 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
242 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
243 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
244 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
245 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
246 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
247 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
248 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
249 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
250 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
251 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
252 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
253 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
254 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
255 ec:c2:b1
256 [usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSAPriv.pem
257 read DSA key
258 Private-Key: (4096 bit)
259   priv:
260     27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
261     16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
262     d8:e7
263   pub:
264     17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
265     cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
266     f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
267     a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
268     be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
269     bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
270     8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
271     6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
272     c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
273     89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
274     12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
275     fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
276     5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
277     b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
278     40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
279     6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
280     35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
281     da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
282     e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
283     7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
284     ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
285     60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
286     3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
287     0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
288     7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
289     30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
290     99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:f0:b4:
291     f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
292     4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
293     a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
294     5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
295     40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
296     6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
297     14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
298     0e:d1
299   P:
300     00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
301     76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
302     28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
```

```
303 89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
304 4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
305 80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
306 69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
307 06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
308 b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
309 c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
310 57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
311 af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
312 8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
313 a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
314 7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
315 f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
316 21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
317 c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
318 82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
319 c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
320 4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
321 cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
322 2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
323 a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
324 fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
325 b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
326 35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
327 bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
328 a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
329 9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
330 2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
331 d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
332 db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
333 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
334 52:f5:e5
335 Q:
336 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
337 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
338 86:b5:11
339 G:
340 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
341 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
342 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
343 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
344 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
345 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
346 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
347 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
348 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
349 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
350 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
351 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
352 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
353 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
354 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
355 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
356 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
357 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
358 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
359 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
360 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
361 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
362 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
363 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
364 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
365 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
366 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
367 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
368 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
369 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
370 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
371 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
372 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
373 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
374 ec:c2:b1
375 [usuario@portatil:~]$ openssl dsa -text -noout -in usuario2/DSApriv.pem.enc
376 read DSA key
377 Enter pass phrase for usuario2/DSApriv.pem.enc:
```

```
378 Private-Key: (4096 bit)
379   priv:
380     27:31:a9:cf:3b:40:21:41:eb:ab:95:6c:ef:01:69:
381     16:33:64:7f:f8:96:7c:0b:d5:15:e4:69:5d:3b:3a:
382     d8:e7
383   pub:
384     17:56:e8:34:9f:24:36:da:b4:81:a6:28:ba:8e:86:
385     cd:6d:c4:e4:b9:62:f7:eb:25:32:80:7c:03:48:ea:
386     f4:79:9f:8d:47:37:6b:ce:38:87:d2:6b:a2:6f:d3:
387     a6:7a:81:1a:9c:50:f7:d2:07:20:a4:5d:3d:35:9b:
388     be:e8:b5:a3:16:67:df:69:fc:9c:5e:4f:5f:c3:32:
389     bd:24:c7:2c:82:e8:05:17:a1:a5:c7:32:9d:83:48:
390     8b:db:73:3b:ae:9f:cc:dd:f9:cb:d9:82:5e:11:36:
391     6e:76:8d:e8:a7:c0:bb:af:94:e2:a0:bc:81:54:f4:
392     c7:22:bb:97:5f:b8:a4:57:0a:be:34:2b:63:e4:5c:
393     89:d6:9b:9b:30:1a:19:4e:9c:88:a0:33:cd:cd:e9:
394     12:8b:3c:2d:8a:c6:45:67:85:c5:3d:89:ec:21:f9:
395     fb:d0:0f:d2:09:e3:19:c1:01:54:a0:32:a5:47:cc:
396     5d:6e:a3:46:ba:88:c7:6e:4a:24:79:6a:b8:ee:13:
397     b4:b6:17:b9:cf:cc:05:42:2d:f5:53:00:9b:4e:9f:
398     40:c3:0f:69:da:5b:e7:3e:ec:60:b9:a5:80:bb:bb:
399     6c:e4:91:9a:38:c0:e2:ee:8b:00:c3:c3:15:38:24:
400     35:c7:47:6d:92:32:ad:07:4d:e0:f8:e2:cb:ca:2b:
401     da:96:a6:67:12:5e:ec:a7:3a:40:7a:2d:b4:e9:2b:
402     e2:99:75:1f:76:8e:09:a1:ef:88:d1:ec:90:2b:5b:
403     7f:a4:3c:6d:99:ce:11:1f:fb:10:63:b5:53:01:a6:
404     ef:9e:c9:5b:db:ea:f7:82:e7:11:2d:3e:20:54:dd:
405     60:81:b1:95:6f:41:cf:93:45:70:73:76:99:8e:50:
406     3f:f8:91:e1:01:d2:e1:55:47:be:d5:89:b4:54:42:
407     0e:76:ea:c9:d9:3e:ee:eb:d6:39:fa:9d:18:dc:34:
408     7f:d1:b0:47:0d:9b:af:fc:f5:3c:bd:76:0b:43:9d:
409     30:8a:38:25:31:74:a1:95:1a:1a:9c:86:ea:d7:f5:
410     99:ca:a5:8f:37:07:08:86:6b:0b:37:60:75:f0:b4:
411     f3:a5:f6:e7:28:08:d1:e4:93:ff:8b:e0:42:d9:30:
412     4c:d8:69:b5:2a:9e:e2:75:de:85:ea:61:b2:44:59:
413     a4:9e:e0:4c:de:8e:98:92:54:ac:0a:64:9a:6f:d8:
414     5c:7b:27:99:66:d2:1f:d2:e6:88:58:d8:48:67:cc:
415     40:d7:83:9d:28:1b:19:82:9f:6f:cb:02:dd:e9:d5:
416     6f:4e:05:28:df:3c:d6:bb:f1:22:31:9f:5a:63:8f:
417     14:4e:36:d1:33:c8:0c:1d:39:e4:3c:93:6a:f3:ef:
418     0e:d1
419   P:
420     00:bb:d3:85:1e:4f:a6:c6:f7:6d:1d:cb:95:90:c3:
421     76:09:74:44:96:32:51:2a:6a:cf:dd:4e:40:d6:87:
422     28:5c:a4:e9:53:8f:41:7a:76:0d:f6:14:26:6f:b4:
423     89:fd:59:02:ac:d6:63:2a:7f:49:cc:6d:91:84:41:
424     4d:33:e8:ec:75:c3:3a:e1:6b:11:45:1a:d6:48:c2:
425     80:e0:0a:75:b3:80:2c:5a:f2:ef:7f:0f:b7:41:ea:
426     69:f6:6b:69:1e:34:09:fe:77:e2:2d:dc:58:ee:48:
427     06:ae:15:27:62:da:05:49:06:90:d9:3b:fe:37:91:
428     b8:f8:5f:88:6a:47:b4:df:9c:8c:f1:54:bd:ce:33:
429     c6:34:0b:61:d7:34:75:95:b7:c4:cc:63:87:e5:1f:
430     57:28:0f:16:04:05:d7:91:31:9f:6b:62:f2:2b:20:
431     af:e3:8a:92:e1:bf:d6:3a:1b:b6:23:c1:b6:c4:24:
432     8c:01:7c:23:8d:c8:52:7c:94:84:a7:4f:dc:30:39:
433     a9:94:82:6b:b9:b3:93:63:a2:45:d7:b1:60:72:76:
434     7b:c6:0c:18:93:d4:5d:a2:6f:c3:b5:98:ac:e9:2e:
435     f0:8b:4e:d8:13:46:a1:83:cc:ed:61:71:ec:c8:8a:
436     21:ba:dd:0b:11:4c:82:cc:9a:85:43:0d:cf:9b:4a:
437     c0:38:dc:46:29:84:e2:aa:83:0c:a9:cb:4a:c9:2d:
438     82:34:51:29:0e:44:c7:cb:a5:b6:1b:c9:cc:68:bf:
439     c6:dc:c0:7d:fe:3a:73:7d:32:b4:2a:ec:89:96:19:
440     4c:ad:6a:2b:f9:b1:70:28:c8:0b:c0:78:06:6a:ca:
441     cc:a0:49:26:be:43:fc:3a:48:51:19:16:31:4b:df:
442     2a:e5:d3:14:eb:3c:58:ed:19:c2:ae:74:a6:36:98:
443     a8:1d:72:0c:c2:d2:f4:92:c2:6f:d4:e2:f5:b9:78:
444     fb:10:80:cf:11:1a:de:41:43:50:32:25:73:a2:fe:
445     b0:bb:3d:0d:3a:12:ee:9e:23:a6:29:b8:50:bb:db:
446     35:95:81:c4:8d:12:00:f1:54:15:82:80:cb:19:d2:
447     bf:dd:ad:38:a4:61:a7:d0:fb:ae:02:39:91:c5:41:
448     a9:8b:63:fa:37:fa:a5:e0:ef:be:be:cb:ed:7d:48:
449     9f:b7:aa:27:4e:fb:15:f6:91:bb:55:98:6a:d0:a1:
450     2a:61:a5:b4:bf:30:e3:6b:fb:4d:9e:54:52:62:b2:
451     d7:b4:da:70:f1:8f:c8:53:b4:45:cd:aa:42:95:47:
452     db:6f:55:cd:6c:e9:bd:7b:b9:e2:86:d4:c5:59:74:
```



```

453 b8:1a:fd:87:52:3f:a1:4a:0f:75:ce:1d:ee:b7:3b:
454 52:f5:e5
455 Q:
456 00:a4:76:9b:c6:0e:d7:1a:d0:8c:ad:15:50:3a:3d:
457 3d:68:e7:74:1e:c7:75:a2:13:20:e8:f9:10:1f:d6:
458 86:b5:11
459 G:
460 00:a8:4e:dc:be:ce:ae:a5:48:16:3f:6b:39:16:1b:
461 77:0a:e9:db:0e:97:7a:08:b9:d5:1e:13:d8:38:d7:
462 0a:68:0b:33:fd:d0:78:3b:2e:cb:ef:bc:1b:77:1c:
463 27:5c:93:2e:c9:a2:a6:47:5d:0c:a5:e1:64:91:c9:
464 8b:97:a2:a1:e4:c8:ac:76:d3:89:56:99:b4:69:bd:
465 83:8a:7b:16:fe:52:29:e3:98:fa:bd:1e:4d:0a:60:
466 79:ae:be:a1:da:32:7a:0b:10:a9:f2:c4:db:6b:de:
467 29:0a:98:a1:82:01:34:2f:ae:90:cc:12:8b:9b:f5:
468 7e:c3:7e:e3:6b:d2:fc:49:b8:ec:34:e2:aa:fd:37:
469 59:31:8a:1e:c2:05:10:5a:3f:8e:f6:82:56:c7:38:
470 44:2e:22:b9:98:af:7e:af:2e:78:b5:83:36:6b:63:
471 cf:19:90:aa:54:1b:6d:43:15:49:17:86:8d:37:9b:
472 9b:04:a3:c9:d1:0c:49:53:b8:a6:01:2d:eb:a2:5d:
473 70:e6:a7:1b:56:54:81:de:1d:ba:b0:2e:f4:b1:48:
474 7d:7d:48:2b:e8:94:4f:62:1f:29:51:43:21:91:08:
475 cb:e0:ae:fe:fb:0c:fe:97:71:9d:20:3d:28:63:67:
476 aa:2c:ab:54:15:10:5b:ee:fd:ba:49:83:a8:04:f6:
477 9d:84:64:b1:8d:de:a2:d1:c3:2f:fb:90:57:52:1f:
478 ad:ab:44:fd:16:59:3f:95:f6:86:26:40:dd:d0:26:
479 2a:76:fd:8d:db:6d:2b:66:28:60:b4:49:e1:66:2d:
480 fe:f7:3d:73:73:67:43:fd:1e:59:20:48:07:aa:5f:
481 62:c1:7b:41:84:d2:15:2b:31:8e:ab:82:ec:90:a8:
482 a7:35:44:8e:9a:06:76:36:00:fd:23:dd:cd:80:be:
483 b0:13:f0:c5:a4:60:00:71:58:f4:bb:ab:8d:a7:2a:
484 fe:34:38:93:63:6a:16:7a:56:d4:32:9d:0a:ec:19:
485 92:8d:db:c7:23:c2:72:f1:ef:0f:57:82:00:c8:c3:
486 6d:6c:a8:df:0e:25:5c:0e:67:92:47:68:81:4f:e1:
487 9c:7b:aa:ea:2c:2d:91:74:28:b1:39:f9:2f:e9:d8:
488 17:da:e4:68:bd:a0:d0:67:d3:62:36:f1:f4:ed:4f:
489 6e:ae:94:9e:62:6f:79:5d:c9:d9:1b:6d:99:e2:aa:
490 c3:58:de:06:fd:5f:7a:1a:65:8a:db:61:21:89:e9:
491 ec:4a:99:7a:7d:a7:48:b8:b9:c8:81:25:6e:32:35:
492 7f:94:c8:c6:3a:17:79:18:20:65:ff:bb:bd:ac:4e:
493 7b:9a:a9:bb:b9:6b:51:18:ea:12:d5:29:cc:06:8e:
494 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.

```

1 [usuario@portatil:~]$ openssl dsa -pubout -outform PEM -in usuario1/Dsakey.pem -out
  usuario1/DsaPub.pem
2 read DSA key
3 writing DSA key
4 [usuario@portatil:~]$
5 [usuario@portatil:~]$ openssl dsa -pubout -outform PEM -in usuario2/Dsakey.pem -out
  usuario2/DsaPub.pem
6 read DSA key
7 writing DSA key
8 [usuario@portatil:~]$ openssl dsa -pubout -in usuario1/Dsakey.pem
9 -----BEGIN PUBLIC KEY-----
10 MIIGRjCCBDkGByqGSM44BAEwggQsAoICAQCdyt7tyYLi7GJ8m/dCsJkV9BZfxZV0
11 tm1z48AtZv3fFFxg/vRnF5MJSSaRFxRLUEn1BgezTFV0EHYujj2EyBIBs3fvLMd
12 X/XDnRvXmh84NY7RD1NDmI2R+oG5rZxhH1ImOynfX3YfoCFKSk6QhT1sRFEdv1HG
13 yk+098zM906CcrMEokY6s9cyaYiaMMoHKVpniRkBgWIF4NH8bAPG7KFFxJfXtL8L
14 mPjAHY6bmtsSmtSAQC6oeG9P8htOKdxnd7TQfpZt3u8LLRqBfQgzHqJmb/KPZf0C
15 1sl+PgRgUpUGnSr2ER3mfD4Lm5gWWQfwb7Sn1lIMI6BFz56ek1l/xV0BUGfRgOL2
16 ysY7Z/FI3DGwnWbGNX26cLitj4AytOCbkwu6ecJ6L6HAuY8II5k+3Ypdx4FepJ6f

```

```

17 YaSLmnsadXyZ2TQv3eDD70j9EtuqC4GZgUjGNKqcHzgyt+B8KyzzeeG9BsX7uPcp
18 /B8asF1iafI02RzbaDUREFRzDf8IwoSxF3hmr41g9ubtkPQTGJoe08RLGuIjRFP7
19 x90yLsrq5TP62FNHvk8pNBLfycUKo5/nqCv9G/zNuuWFFU2TTIgH0yBdF3H6C+L7
20 gWNe+McSuCDHsgy1EiRAURFihIqw8eTcqix6/t7IPSpkC4Gh1sRkhqvS8021gcck
21 zUWkgpsLzIzJBwIhAPypEJTMxiN19zjGM81+zDBM2LVfkJDP4JYVQ5qle55DAoIC
22 ABwBBu9opARxzS4MN3JlgbqNv3uk07nSOK2stqNJTUXizP5r4qnmv2qUsAH+1kNZ
23 hJcwRf1Gq06Fz761PgRfBzdh7q4M1DSXg12hc9Sffsu9A4Eiz8ZFMWHpWuYm+24g
24 uErXFDSBGkxFHCKyMYfzlgMkhooBSnFRmS93a+HpV8DkSst+5qkXAxPnIpi/seV4
25 F8Qx8jK34nibbLVrJwMbxE32BDy7KBFs6615fz46PXsYEclBIB1zoypu/s95UK5h
26 egz+5z6VImad3wIjxrNOTUQ+Z5jq8ZboN6qcTqjZgDwz4AnXUHGZDoWJ1X6zk+kw
27 1rUW00aWfvBUX2mva00e143mD7a6AMigQJsOjj26p05g/wI2JB42dEZIzJXHrW3S
28 MHE0IMH1kEfXpmwefC0inbqgPij07eUsZfndYF6KXSJhUZdGB7kt8chHEWIZS13F
29 baovx1aXugFcuatHtxdMSF9+cesyoxWXzz4J2YzUuBAasy/08jCnJjxCuP6Uu52Fs
30 bnmcTS73+STRZQMxvQT8+Z+9Iw2mr9BNyhhM1wbMDT/7wPo3GcVntLLTmIbF6GY
31 iYy5yw23f6JxqH4HwjTJONXua5dCr4WuEejG8Rc/rh2m5SCJixv20JP2KQ20sNJL
32 USwJrvCPQevGB1d9t0uenc7f+Th4x6aKSpGHBoOfDA90A4ICBQACggIARA9MwnOy
33 +RM1xK0iSypg1mZjCh9dqg+zuFga3FvB8e85KBlg5kQIM8kmmTAKUqjZ5yhGRyla
34 13lvYplmB6hrw3DU9ufjQyXnhLHZCexZjIBA0i1AXJPumJ6wN/x0kj7E1N4W1NbL
35 ToF/sbEc/pH8xjHlRdW/ZmiF0m8xIYE2bB5tSPtj9sp/vShRkiI7upYJijuHNX9L
36 Aqavg6zdg98BAmidGwAsBxjdwUqLgHasWyRF09FRhIUwF34iFpd5Bw0fbbhekQ3k
37 oAplamxrAEySI9TIVTirAi1Fg4Z+L4A6RnVNg14R1G8WMKzVNCbHhJnxmYLxkq7
38 7ht8CihwErVSxRomxdkkh2p3LZZ+0wfbAQaCuxyrFi6DvSJYsSXwWXAQ/vsknY1
39 WGuMmM0/z7USbKqd0JeI4x2wzG/u4YH0qm60iJpGmW1xobv/vKIuVQCQ5HGe+irk
40 iq9nmdHPj1L1kJwP34/4V9qz5PYR22U0VPGLi8Y8KKBhpmwAzciNo50MFgd891Q
41 l4iKylHsqIxeSibBbskxzJsZOMXus5mTbH8KdU2Vkojosv2ui9F0savhpTAADT4/
42 HF6UWCb4cKgm/KPvHIF0mGnVix6U6tWBWKiwbJEQ/7/2qTwQ/n70+dZSOk3IV4A3
43 R6UGJd2u8zXy5dsSEEESE5SZCQ78CtGeouY=
44 -----END PUBLIC KEY-----
45 [usuario@portatil:~]$ openssl dsa -pubout -in usuario2/DSAkey.pem
46 -----BEGIN PUBLIC KEY-----
47 MIIGRjCCBDkGByqGSM44BAEwggQsAoICAQCdyt7tyYLi7GJ8m/dCsJkV9BZfxZV0
48 tm1z48AtZv3fFFxg/vRnF5MJSSaRfXRLUHen1BgezTFV0EHYuj2EyBIBs3fvLMd
49 X/XDnRvxxmh84NY7RD1NDmI2R+oG5rZxhHlImOynfX3YfoCFKSk6QhT1sRFEdv1HG
50 yk+098zm906CcrMEokY6s9cyaYiaMMoHKVpniRkBgWIF4N88bAPG7KFFxJfXtL8L
51 mPjAHY6bmtsSmtSAQC6oeG9P8htOKdxnd7TQfpZt3u81LRqBfQgzHqJmb/KPZf0C
52 1s1+PgRgUpUGnSr2ER3mfD4Lm5gWWQfwb7Sn1lIMI6BFz56ek1l/xV0BUGfRgOL2
53 ysY7Z/FI3DGwnWbGNX26cL1tj4AytOCbkwu6ecJ6L6HAUy8II5k+3Ypdx4FepJ6f
54 YaSLmnsadXyZ2TQv3eDD70j9EtuqC4GZgUjGNKqcHzgyt+B8KyzzeeG9BsX7uPcp
55 /B8asF1iafI02RzbaDUREFRzDf8IwoSxF3hmr41g9ubtkPQTGJoe08RLGuIjRFP7
56 x90yLsrq5TP62FNHvk8pNBLfycUKo5/nqCv9G/zNuuWFFU2TTIgH0yBdF3H6C+L7
57 gWNe+McSuCDHsgy1EiRAURFihIqw8eTcqix6/t7IPSpkC4Gh1sRkhqvS8021gcck
58 zUWkgpsLzIzJBwIhAPypEJTMxiN19zjGM81+zDBM2LVfkJDP4JYVQ5qle55DAoIC
59 ABwBBu9opARxzS4MN3JlgbqNv3uk07nSOK2stqNJTUXizP5r4qnmv2qUsAH+1kNZ
60 hJcwRf1Gq06Fz761PgRfBzdh7q4M1DSXg12hc9Sffsu9A4Eiz8ZFMWHpWuYm+24g
61 uErXFDSBGkxFHCKyMYfzlgMkhooBSnFRmS93a+HpV8DkSst+5qkXAxPnIpi/seV4
62 F8Qx8jK34nibbLVrJwMbxE32BDy7KBFs6615fz46PXsYEclBIB1zoypu/s95UK5h
63 egz+5z6VImad3wIjxrNOTUQ+Z5jq8ZboN6qcTqjZgDwz4AnXUHGZDoWJ1X6zk+kw
64 1rUW00aWfvBUX2mva00e143mD7a6AMigQJsOjj26p05g/wI2JB42dEZIzJXHrW3S
65 MHE0IMH1kEfXpmwefC0inbqgPij07eUsZfndYF6KXSJhUZdGB7kt8chHEWIZS13F
66 baovx1aXugFcuatHtxdMSF9+cesyoxWXzz4J2YzUuBAasy/08jCnJjxCuP6Uu52Fs
67 bnmcTS73+STRZQMxvQT8+Z+9Iw2mr9BNyhhM1wbMDT/7wPo3GcVntLLTmIbF6GY
68 iYy5yw23f6JxqH4HwjTJONXua5dCr4WuEejG8Rc/rh2m5SCJixv20JP2KQ20sNJL
69 USwJrvCPQevGB1d9t0uenc7f+Th4x6aKSpGHBoOfDA90A4ICBQACggIABKiaBJgz
70 GwnYhiNMyoAv3h7GHmxr2MnoS2ju+lg4Q5nYTQQA5teQ7Im1NoKeHCIG/NL3xtcN
71 zzQxnS8FQYET1mGE9rRQuZ4uhyEUWjG4aHLPJNn8pzorZjfs+wq8SgsHFz37dvNG
72 5krhra6CLBp/MMKIdbYdx7xNceZ45IXyZDRx6GKbBWD9wLS+C710bVG83hyjIHf
73 baOMt1NvKz0B2mH9HwP+snxZ8Imrtj+vd+ihl7WT+8U5T9mnAnVcGmJ2+pvq6aFY
74 qgzWVF2MFSZTR0tfCuSaskgTxPd3V90x/Ct4lav5Fd0oG2NM0xTGzXK0XWzGxzB
75 ebHYw3JVq9b/HLOZc83F1rVEIJA1s10h1XbMTDdm70f9WgXM9w21d1GJ9P3c3q0+
76 fwcEhM50rofL3LG4szbM8DxP1CVw/A011/lnTH+1mE15nK6LKG0vm+TNhbNVL6ts
77 wfd1QHEN0ViY3aaIUQtvbHXpVSCalX0wZk3VE2qCTu05GfV+zh9zpuAe4nDVqec5
78 2b0u4Ev9Z40m/HSNQHhqvVyG+95mucj/xpfaIKS8CyZ/FaB4jcdKNFmfgS+KtgFTb
79 83b2pcdnJVmdnfatZUxDRamekRCcZ6zQZcdhwglIPAtIhIbalT61h8uXzSpMNECE
80 7ogh5Js4nHqkQ2xa07AzHsaMxsw3etduXXA=
81 -----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.

```

1 [usuario@portatil:~]$ dd bs=128 count=1 </dev/urandom > /tmp/message
2 1+0 registros leídos
3 1+0 registros escritos
4 128 bytes copied, 0,00019602 s, 653 kB/s
5 [usuario@portatil:~]$ hexdump usuario1/message
6 0000000 8886 8ea6 ed2a 67d7 0226 10a8 bc18 8ac6
7 0000010 e85a 7f09 70a4 d8a6 a490 d5c9 f01a 36a1
8 0000020 4a1a 4817 3aff 5899 b4a8 dd8c c207 5347
9 0000030 1995 2dc8 42ea f9d5 d2c0 081c fcf0 fc35
10 0000040 57c2 95cc 38f7 feb8 4bdf 004d 8fab cda1
11 0000050 7069 67e0 dc09 285b f6bb 7a97 6983 1339
12 0000060 159d 89ad 345e 9904 fce3 4a9d 639f 4a71
13 0000070 c59b 767a 016f e36f b7e6 0556 0d7b b1e2
14 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.

```

1 [usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario1/DSAkey.pem -in /tmp/message -
  out /tmp/message.sign
2 [usuario@portatil:~]$ hexdump /tmp/message.sign
3 0000000 4530 2002 e70b 6ea7 dc3f 0776 53a1 7fa4
4 0000010 8546 5c49 2e2c 1a5d 56d3 3d7a 7463 d537
5 0000020 0477 5e5c 2102 da00 875d 6822 b3d8 1530
6 0000030 3376 7882 a13d 6227 6e23 f5a9 ffac 940d
7 0000040 7335 63de e3e6 00fd
8 0000047
9 [usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario2/DSAkey.pem -in /tmp/message -
  out /tmp/message.sign
10 [usuario@portatil:~]$ hexdump /tmp/message.sign
11 0000000 4530 2002 e15a 1702 283f dccf bb78 36dd
12 0000010 1d81 d630 37dc 5113 4159 b719 0b0e 7cd0
13 0000020 9c1a f1d4 2102 8400 ac17 f17e d59b 4777
14 0000030 dbc7 8a62 6892 3eff 68cc 30d4 0c15 7aa4
15 0000040 f834 5566 35e3 0031
16 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.

```

1 [usuario@portatil:~]$ dd bs=32 count=1 </dev/urandom > /tmp/extra
2 1+0 registros leídos
3 1+0 registros escritos
4 32 bytes copied, 2,5534e-05 s, 1,3 MB/s
5 [usuario@portatil:~]$ cat /tmp/message > /tmp/message2
6 [usuario@portatil:~]$ cat /tmp/extra >> /tmp/message2
7 [usuario@portatil:~]$ hexdump /tmp/message
8 0000000 21b1 276b 8b08 1d98 73a4 653a f2e4 a87b

```

```

9 0000010 903b 196d 52e6 7441 d11a 4a76 fcbd 98c5
10 0000020 d178 582b 1456 af12 63de e8ef 7af5 e61f
11 0000030 cd33 2252 6ba6 f11a 46f9 55c8 a7f6 1931
12 0000040 150d c9f5 be05 501d a3cf 9747 c894 2eff
13 0000050 5bf3 f327 bc8b 33fe 48c1 d3d8 bae3 b879
14 0000060 ce82 a841 d7bd c668 a7b7 7135 d513 b4d7
15 0000070 3358 ec34 4485 8d1f 5d56 77e2 e45b 6540
16 0000080
17 [usuario@portatil:~]$ hexdump /tmp/message2
18 0000000 21b1 276b 8b08 1d98 73a4 653a f2e4 a87b
19 0000010 903b 196d 52e6 7441 d11a 4a76 fcbd 98c5
20 0000020 d178 582b 1456 af12 63de e8ef 7af5 e61f
21 0000030 cd33 2252 6ba6 f11a 46f9 55c8 a7f6 1931
22 0000040 150d c9f5 be05 501d a3cf 9747 c894 2eff
23 0000050 5bf3 f327 bc8b 33fe 48c1 d3d8 bae3 b879
24 0000060 ce82 a841 d7bd c668 a7b7 7135 d513 b4d7
25 0000070 3358 ec34 4485 8d1f 5d56 77e2 e45b 6540
26 0000080 eb85 7f8b 6c2a 5a79 4b1d 9b77 a479 254d
27 0000090 1f28 1513 e9c3 bb50 de94 44c3 4b07 b78b
28 00000a0
29 [usuario@portatil:~]$ openssl pkeyutl -sign -inkey usuario1/DSAkey.pem -in /tmp/message -
    out /tmp/message.sign
30 [usuario@portatil:~]$ openssl pkeyutl -verify -inkey usuario1/DSAkey.pem -sigfile /tmp/
    message.sign -in /tmp/message
31 Signature Verified Successfully
32 [usuario@portatil:~]$ openssl pkeyutl -verify -inkey usuario1/DSAkey.pem -sigfile /tmp/
    message.sign -in /tmp/message2
33 Signature Verified Successfully

```

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

```

1 [usuario@portatil:~]$ openssl dgst -sha384 -c -out usuario1/DSAPub.pem.sha384 usuario1/
    DSAPub.pem
2 [usuario@portatil:~]$ cat usuario1/DSAPub.pem.sha384
3 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.

```

1 [usuario@portatil:~]$ openssl dgst -c -binary -sha1 -out /tmp/message2.sha1 /tmp/message2
2 [usuario@portatil:~]$ hexdump /tmp/message2.sha1
3 0000000 2b5e cd96 71c2 d8cb 33c2 18c1 f61c 030a
4 0000010 0c5a 1efa
5 0000014
6 [usuario@portatil:~]$ ls -la /tmp/message2.sha1
7 -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.

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

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

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

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

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

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

```
1 [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:

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

```
1 [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>.