PRACTICA 3

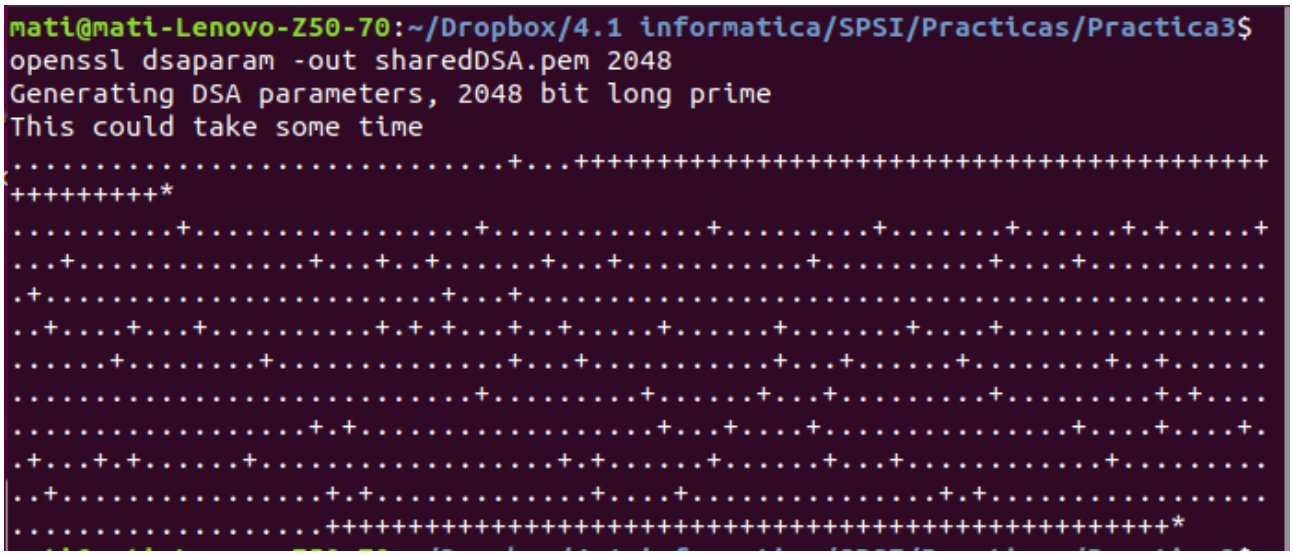
Protocolos Criptográficos

Matilde Cabrera González

Tareas por realizar:

Para esta práctica, deberéis simular la presencia de dos usuarios, por lo que la generación de claves sera doble, incluyendo las reutilizadas de la practica anterior.

1. (0,5 puntos) Generad un archivo sharedDSA.pem que contenga los parámetros. Mostrad los valores.



```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsaparam -in sharedDSA.pem -text -noout
    P:
        00:9c:c7:85:8c:59:00:f4:7b:44:a7:d9:07:0a:b7:
        fd:e8:84:56:24:4e:4d:ff:a8:12:9d:1a:ea:2a:a7:
        17:8b:72:f7:97:c1:65:5d:8d:5c:a6:de:8f:23:4e:
        f2:de:cb:f6:7e:27:d0:a8:e6:5c:77:f8:0f:d1:9d:
        fd:80:64:d4:99:da:cb:ba:0d:03:6a:9b:70:6b:a0:
        a6:a1:57:eb:d0:58:57:d8:74:5a:9e:de:66:80:39:
        94:40:da:83:94:8f:bd:14:fb:b0:75:78:cd:b0:18:
        91:b1:d7:7c:c9:d1:3a:20:34:0d:dc:ca:a5:31:f1:
        aa:b6:f0:57:be:9e:34:56:29:0d:04:22:b1:2b:4e:
        0f:60:3c:8e:32:c2:ea:93:81:11:ff:4b:fc:e6:dd:
        39:07:53:5a:5e:e1:2f:cc:89:24:98:52:88:8a:33:
        a5:fb:bf:71:56:12:c8:14:99:32:5c:13:c0:50:7d:
        b6:df:52:e5:bf:ef:f9:68:74:63:d3:28:a8:d2:ff:
        67:3e:1f:49:41:79:84:19:a3:e1:5c:54:f8:ed:12:
        d6:ca:32:30:54:96:2d:54:3b:55:b7:c8:56:8a:08:
        32:30:7c:02:7d:50:a1:a0:40:8d:b2:07:1c:ab:87:
        ff:ec:14:c6:be:ce:d0:71:fc:3d:49:fa:ca:cf:52:
        46:33
    Q:
        00:e8:f0:eb:d2:45:b8:6d:39:49:65:da:7d:6f:97:
        f3:4f:4d:8d:72:84:dc:2b:ef:e0:66:04:de:1a:82:
        ec:c7:75
    G:
        00:85:fc:38:2c:13:24:4d:69:78:12:01:3c:1d:16:
        b6:e9:5c:64:98:a3:06:8b:d0:a5:04:23:70:f7:bb:
        d7:d7:46:30:37:37:d5:50:86:44:15:04:e3:7e:bd:
        29:dc:a5:6e:fa:0d:ce:1b:8d:5b:8e:85:03:cc:3a:
        6c:a6:41:2d:b1:13:16:85:71:46:52:43:2e:84:1e:
        0a:7f:96:24:6d:cb:a9:32:f0:38:69:ad:46:aa:95:
        5f:97:60:e9:9f:9e:eb:e1:41:5d:c7:82:4f:1b:55:
        10:f8:2b:e5:2f:0c:4c:bb:99:f7:83:ff:fa:f6:cb:
        5f:55:bc:21:3b:84:78:ef:eb:31:5e:ee:be:00:48:
        eb:eb:a3:32:f0:b8:07:d1:0d:25:75:e3:8e:e1:b6:
        1d:7a:09:a3:4f:20:c2:68:9d:16:eb:d5:05:c7:a5:
        47:b6:56:51:6a:d7:e9:0c:35:e5:88:b8:94:89:ab:
        07:b3:2e:a0:f3:a9:77:91:bd:a3:83:ce:95:b9:ed:
        48:98:14:a3:3e:61:5a:4b:91:35:26:05:21:ba:4f:
        0c:a2:80:20:7a:ed:7d:92:a7:a6:9f:88:a5:1a:00:
        37:9f:66:9b:20:00:a4:c0:16:a1:3e:33:82:40:2e:
        e4:c4:46:61:90:e0:0e:37:79:c3:a3:de:3c:04:22:
        a7:52
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

2. (0,5 puntos) Generad dos parejas de claves para los parámetros anteriores. La claves se almacenaran en los archivos <nombre>DSAkey.pem y <apellido>DSAkey.p No es necesario protegerlas por contraseña.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl gendsa -out matiDSAkey.pem sharedDSA.pem
Generating DSA key, 2048 bits
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl gendsa -out cabreraDSAkey.pem sharedDSA.pem
Generating DSA key, 2048 bits
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
cat matiDSAkey.pem
-----BEGIN DSA PRIVATE KEY-----
MIIDVgIBAAKCAQEAnMeFjFkA9HtEp9kHCrf96IRWJE5N/6gSnRrqKqcXi3L3l8Fl
XY1cpt6PI07y3sv2fifQqOZcd/gP0Z39gGTUmdrLug0Daptwa6CmoVfr0FhX2HRa
nt5mgDmUQNqDlI+9FPuwdXjNsBiRsdd8ydE6IDQN3MqlMfGqtvBXvp40VikNBCKx
K04PYDyOMsLqk4ER/0v85t05B1NaXuEvzIkkmFKIijOl+79xVhLIFJkyXBPAUH22
31Llv+/5aHRj0yio0v9nPh9JQXmEGaPhXFT47RLWyjIwVJYtVDtVt8hWiggyMHwC
fVChoECNsgccq4f/7BTGvs7Qcfw9SfrKz1JGMwIhAOjw69JFuG05SWXafW+X809N
jXKE3Cvv4GYE3hqC7Md1AoIBAQCF/DgsEyRNaXgSATwdFrbpXGSYowaL0KUEI3D3
u9fXRjA3N9VQhkQVBON+vSncpW76Dc4bjVuOhQPMOmymQS2xExaFcUZSQy6EHgp/
liRty6ky8DhprUaqlV+XYOmfnuvhQV3Hgk8bVRD4K+UvDEy7mfeD//r2y19VvCE7
hHjv6zFe7r4ASOvrozLwuAfRDSV1447hth16CaNPIMJonRbr1QXHpUe2VlFq1+kM
NeWIuJSJqwezLqDzqXeRvaODzpW57UiYFKM+YVpLkTUmBSG6TwyigCB67X2Sp6af
iKUaADefZpsgAKTAFqE+M4JALuTERmGQ4A43ecOj3jwEIqdSAoIBAFzrJo8jdCKj
U3QEYRzVCX0ZubMxepD1RIFc3xLzfomIypClK7Eqz35+C9NfdhGLHaFpsnkcg/QH
AM0m5MlBXU7reN5+RTXgoeMDcSU7q5ZD+roI7lqbLI5qm1nKlNc+7QsYxjPtj/7c
FB6EbyK4WASTMGAqVE8SBb4hhmWohrhUECZfTK9020HRZGoDIt537ZEVyQruKbWa
iTPse0rzMZD7CYrxNBfAbxYYzkVc5cRAeB2RZOpCY7iM6dzxgnI5E4x+G2jGYvpt
o75idy5wHw32KGg7UNZlktqjqptU8Bm4y5XRKuLJzXbNd38P7gvkissDTw4nRTK4
ILg2Y5wFXrYCIH/rkzIxkJgSc6U+/K0sdbIPG6efL6HxWBl53wLUk9vO
-----END DSA PRIVATE KEY-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
cat cabreraDSAkey.pem
-----BEGIN DSA PRIVATE KEY-----
MIIDVgIBAAKCAQEAnMeFjFkA9HtEp9kHCrf96IRWJE5N/6gSnRrqKqcXi3L3l8Fl
XY1cpt6PI07y3sv2fifQqOZcd/gP0Z39gGTUmdrLug0Daptwa6CmoVfr0FhX2HRa
nt5mgDmUQNqDlI+9FPuwdXjNsBiRsdd8ydE6IDQN3MqlMfGqtvBXvp40VikNBCKx
K04PYDyOMsLqk4ER/0v85t05B1NaXuEvzIkkmFKIijOl+79xVhLIFJkyXBPAUH22
31Llv+/5aHRj0yio0v9nPh9JQXmEGaPhXFT47RLWyjIwVJYtVDtVt8hWiggyMHwC
fVChoECNsgccq4f/7BTGvs7Qcfw9SfrKz1JGMwIhAOjw69JFuG05SWXafW+X809N
jXKE3Cvv4GYE3hqC7Md1AoIBAQCF/DgsEyRNaXgSATwdFrbpXGSYowaL0KUEI3D3
u9fXRjA3N9VQhkQVBON+vSncpW76Dc4bjVuOhQPMOmymQS2xExaFcUZSQy6EHgp/
liRty6ky8DhprUaqlV+XYOmfnuvhQV3Hgk8bVRD4K+UvDEy7mfeD//r2y19VvCE7
hHjv6zFe7r4ASOvrozLwuAfRDSV1447hth16CaNPIMJonRbr1QXHpUe2VlFq1+kM
NeWIuJSJqwezLqDzqXeRvaODzpW57UiYFKM+YVpLkTUmBSG6TwyigCB67X2Sp6af
iKUaADefZpsgAKTAFqE+M4JALuTERmGQ4A43ecOj3jwEIqdSAoIBAG/wWmAy/2J2
MuDrCePceixStFZSrwJH1SzvWKOX176aLgjjkQC39vqy16rYbAUnhLdKl+s5JPje
AKVB834dJUq0dwwBBEJdZ6F+iJg8ublhJSDJKnwE9xq1MWn5beDXe/D+ijdUHgvV
Qep9tlUfzJ7s/QIKMSaNXcQEtqnLMwSz4KsxW+KAI1B89GDmETs3Kk9JS1M9azM4
/mQ7xVuwo/vVCCXPITaW/r0gC3m+A5PEFPXwvJeYO0AIxaRVy0AdGw5Mok6Z1htz
epHr4v45QBv0/0LVOAFux9SuQobepVH8kOAmPQB8FKk6xuSJcV7oSMpzlbNPnQ1V
GYQKxmuOCHACICKUVPplOWiz5t5fDPi52UC53dRDi6R5omkWpcydazDK
-----END DSA PRIVATE KEY-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

3. (0,5 puntos) “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 .

Extraemos la clave privada y protegemos el archivo cifrando con AES-128 con contraseña “0123456789”, en ambos archivos:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in matiDSAkey.pem -out matiDSApriv.pem -aes128
read DSA key
writing DSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in matiDSApriv.pem -text -noout
read DSA key
Enter pass phrase for matiDSApriv.pem:
Private-Key: (2048 bit)
priv:
    7f:eb:93:32:31:90:98:12:73:a5:3e:fc:ad:2c:75:
    b2:0f:1b:a7:9f:2f:a1:f1:58:19:79:df:02:d4:93:
    db:ce
pub:
    5c:eb:26:8f:23:74:22:a3:53:74:04:61:1c:d5:09:
    7d:19:b9:b3:31:7a:90:f5:44:81:5c:df:12:f3:7e:
    89:88:ca:90:a5:2b:b1:2a:cf:7e:7e:0b:d3:5f:76:
    11:8b:1d:a1:69:b2:79:1c:83:f4:07:00:cd:26:e4:
    c9:41:5d:4e:eb:78:de:7e:45:35:e0:a1:e3:03:71:
    25:3b:ab:96:43:fa:ba:08:ee:5a:9b:2c:8e:6a:9b:
    59:ca:94:d7:3e:ed:0b:18:c6:33:ed:8f:fe:dc:14:
    1e:84:6f:22:b8:58:04:93:30:60:2a:54:4f:12:05:
    be:21:86:65:a8:86:b8:54:10:26:5f:4c:af:74:db:
    41:d1:64:6a:03:22:de:77:ed:91:15:c9:0a:ee:29:
    b5:9a:89:33:ec:7b:4a:f3:31:90:fb:09:8a:f1:34:
    17:c0:6f:16:18:ce:45:5c:e5:c4:40:78:1d:91:64:
    ea:42:63:b8:8c:e9:dc:f1:82:72:39:13:8c:7e:1b:
    68:c6:62:fa:6d:a3:be:62:77:2e:70:1f:0d:f6:28:
    68:3b:50:d6:65:92:da:a3:aa:9b:54:f0:19:b8:cb:
    95:d1:2a:e2:c9:cd:76:cd:77:7f:0f:ee:0b:e4:8a:
    cb:03:4f:0e:27:45:32:b8:20:b8:36:63:9c:05:5e:
    b6
```

```
P:
    00:9c:c7:85:8c:59:00:f4:7b:44:a7:d9:07:0a:b7:
    fd:e8:84:56:24:4e:4d:ff:a8:12:9d:1a:ea:2a:a7:
    17:8b:72:f7:97:c1:65:5d:8d:5c:a6:de:8f:23:4e:
    f2:de:cb:f6:7e:27:d0:a8:e6:5c:77:f8:0f:d1:9d:
    fd:80:64:d4:99:da:cb:ba:0d:03:6a:9b:70:6b:a0:
    a6:a1:57:eb:d0:58:57:d8:74:5a:9e:de:66:80:39:
    94:40:da:83:94:8f:bd:14:fb:b0:75:78:cd:b0:18:
    91:b1:d7:7c:c9:d1:3a:20:34:0d:dc:ca:a5:31:f1:
    aa:b6:f0:57:be:9e:34:56:29:0d:04:22:b1:2b:4e:
    0f:60:3c:8e:32:c2:ea:93:81:11:ff:4b:fc:e6:dd:
    39:07:53:5a:5e:e1:2f:cc:89:24:98:52:88:8a:33:
    a5:fb:bf:71:56:12:c8:14:99:32:5c:13:c0:50:7d:
    b6:df:52:e5:bf:ef:f9:68:74:63:d3:28:a8:d2:ff:
    67:3e:1f:49:41:79:84:19:a3:e1:5c:54:f8:ed:12:
    d6:ca:32:30:54:96:2d:54:3b:55:b7:c8:56:8a:08:
    32:30:7c:02:7d:50:a1:a0:40:8d:b2:07:1c:ab:87:
    ff:ec:14:c6:be:ce:d0:71:fc:3d:49:fa:ca:cf:52:
    46:33
Q:
    00:e8:f0:eb:d2:45:b8:6d:39:49:65:da:7d:6f:97:
    f3:4f:4d:8d:72:84:dc:2b:ef:e0:66:04:de:1a:82:
    ec:c7:75
G:
    00:85:fc:38:2c:13:24:4d:69:78:12:01:3c:1d:16:
    b6:e9:5c:64:98:a3:06:8b:d0:a5:04:23:70:f7:bb:
    d7:d7:46:30:37:37:d5:50:86:44:15:04:e3:7e:bd:
    29:dc:a5:6e:fa:0d:ce:1b:8d:5b:8e:85:03:cc:3a:
    6c:a6:41:2d:b1:13:16:85:71:46:52:43:2e:84:1e:
    0a:7f:96:24:6d:cb:a9:32:f0:38:69:ad:46:aa:95:
    5f:97:60:e9:9f:9e:eb:e1:41:5d:c7:82:4f:1b:55:
    10:f8:2b:e5:2f:0c:4c:bb:99:f7:83:ff:fa:f6:cb:
    5f:55:bc:21:3b:84:78:ef:eb:31:5e:ee:be:00:48:
    eb:eb:a3:32:f0:b8:07:d1:0d:25:75:e3:8e:e1:b6:
    1d:7a:09:a3:4f:20:c2:68:9d:16:eb:d5:05:c7:a5:
    47:b6:56:51:6a:d7:e9:0c:35:e5:88:b8:94:89:ab:
    07:b3:2e:a0:f3:a9:77:91:bd:a3:83:ce:95:b9:ed:
    48:98:14:a3:3e:61:5a:4b:91:35:26:05:21:ba:4f:
    0c:a2:80:20:7a:ed:7d:92:a7:a6:9f:88:a5:1a:00:
    37:9f:66:9b:20:00:a4:c0:16:a1:3e:33:82:40:2e:
    e4:c4:46:61:90:e0:0e:37:79:c3:a3:de:3c:04:22:
    a7:52
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in cabreraDSAkey.pem -out cabreraDSApriv.pem -aes128
read DSA key
writing DSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in cabreraDSApriv.pem -text -noout
read DSA key
Enter pass phrase for cabreraDSApriv.pem:
Private-Key: (2048 bit)
priv:
    22:94:54:fa:65:39:68:b3:e6:de:5f:0c:f8:b9:d9:
    40:b9:dd:d4:43:8b:a4:79:a2:69:16:a5:cc:9d:6b:
    30:ca
pub:
    6f:f0:5a:60:32:ff:62:76:32:e0:eb:09:e3:dc:7a:
    2c:52:b4:56:52:af:02:47:d5:2c:ef:58:a3:97:d7:
    be:9a:2e:08:e3:91:00:b7:f6:fa:b2:d7:aa:d8:6c:
    05:27:84:b7:4a:97:eb:39:24:f8:de:00:a5:41:f3:
    7e:1d:25:4a:b4:77:0c:01:04:42:5d:67:a1:7e:88:
    98:3c:b9:b9:61:25:20:c9:2a:7c:04:f7:1a:b5:31:
    69:f9:6d:e0:d7:7b:f0:fe:8a:37:54:1e:0b:d5:41:
    ea:7d:b6:55:1f:cc:9e:ec:fd:02:0a:31:26:8d:5d:
    c4:04:b6:a9:cb:33:04:b3:e0:ab:31:5b:e2:80:23:
    50:7c:f4:60:e6:11:3b:37:2a:4f:49:4b:53:3d:6b:
    33:38:fe:64:3b:c5:5b:b0:a3:fb:d5:08:25:cf:21:
    36:96:fe:bd:20:0b:79:be:03:93:c4:14:f5:f0:bc:
    97:98:3b:40:08:c5:a4:55:cb:40:1d:1b:0e:4c:a2:
    4e:99:d6:1b:73:7a:91:eb:e2:fe:39:40:1b:f4:ff:
    42:d5:38:01:6e:c7:d4:ae:42:86:de:a5:51:fc:90:
    e0:26:3d:00:7c:14:a9:3a:c6:e4:89:71:5e:e8:48:
    ca:73:95:b3:4f:9d:0d:55:19:84:0a:c6:6b:8e:08:
    70
P:
    00:9c:c7:85:8c:59:00:f4:7b:44:a7:d9:07:0a:b7:
    fd:e8:84:56:24:4e:4d:ff:a8:12:9d:1a:ea:2a:a7:
    17:8b:72:f7:97:c1:65:5d:8d:5c:a6:de:8f:23:4e:
    f2:de:cb:f6:7e:27:d0:a8:e6:5c:77:f8:0f:d1:9d:
    fd:80:64:d4:99:da:cb:ba:0d:03:6a:9b:70:6b:a0:
    a6:a1:57:eb:d0:58:57:d8:74:5a:9e:de:66:80:39:
    94:40:da:83:94:8f:bd:14:fb:b0:75:78:cd:b0:18:
    91:b1:d7:7c:c9:d1:3a:20:34:0d:dc:ca:a5:31:f1:
    aa:b6:f0:57:be:9e:34:56:29:0d:04:22:b1:2b:4e:
    0f:60:3c:8e:32:c2:ea:93:81:11:ff:4b:fc:e6:dd:
    39:07:53:5a:5e:e1:2f:cc:89:24:98:52:88:8a:33:
    a5:fb:bf:71:56:12:c8:14:99:32:5c:13:c0:50:7d:
    b6:df:52:e5:bf:ef:f9:68:74:63:d3:28:a8:d2:ff:
    67:3e:1f:49:41:79:84:19:a3:e1:5c:54:f8:ed:12:
    d6:ca:32:30:54:96:2d:54:3b:55:b7:c8:56:8a:08:
    32:30:7c:02:7d:50:a1:a0:40:8d:b2:07:1c:ab:87:
    ff:ec:14:c6:be:ce:d0:71:fc:3d:49:fa:ca:cf:52:
    46:33
Q:
    00:e8:f0:eb:d2:45:b8:6d:39:49:65:da:7d:6f:97:
    f3:4f:4d:8d:72:84:dc:2b:ef:e0:66:04:de:1a:82:
    ec:c7:75
```

```
G:
    00:85:fc:38:2c:13:24:4d:69:78:12:01:3c:1d:16:
    b6:e9:5c:64:98:a3:06:8b:d0:a5:04:23:70:f7:bb:
    d7:d7:46:30:37:37:d5:50:86:44:15:04:e3:7e:bd:
    29:dc:a5:6e:fa:0d:ce:1b:8d:5b:8e:85:03:cc:3a:
    6c:a6:41:2d:b1:13:16:85:71:46:52:43:2e:84:1e:
    0a:7f:96:24:6d:cb:a9:32:f0:38:69:ad:46:aa:95:
    5f:97:60:e9:9f:9e:eb:e1:41:5d:c7:82:4f:1b:55:
    10:f8:2b:e5:2f:0c:4c:bb:99:f7:83:ff:fa:f6:cb:
    5f:55:bc:21:3b:84:78:ef:eb:31:5e:ee:be:00:48:
    eb:eb:a3:32:f0:b8:07:d1:0d:25:75:e3:8e:e1:b6:
    1d:7a:09:a3:4f:20:c2:68:9d:16:eb:d5:05:c7:a5:
    47:b6:56:51:6a:d7:e9:0c:35:e5:88:b8:94:89:ab:
    07:b3:2e:a0:f3:a9:77:91:bd:a3:83:ce:95:b9:ed:
    48:98:14:a3:3e:61:5a:4b:91:35:26:05:21:ba:4f:
    0c:a2:80:20:7a:ed:7d:92:a7:a6:9f:88:a5:1a:00:
    37:9f:66:9b:20:00:a4:c0:16:a1:3e:33:82:40:2e:
    e4:c4:46:61:90:e0:0e:37:79:c3:a3:de:3c:04:22:
    a7:52
```

4. (0,5 puntos) 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 .

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in matiDSAkey.pem -pubout -out matiDSApub.pem
read DSA key
writing DSA key
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in matiDSApub.pem -text -noout -pubin
read DSA key
pub:
    5c:eb:26:8f:23:74:22:a3:53:74:04:61:1c:d5:09:
    7d:19:b9:b3:31:7a:90:f5:44:81:5c:df:12:f3:7e:
    89:88:ca:90:a5:2b:b1:2a:cf:7e:7e:0b:d3:5f:76:
    11:8b:1d:a1:69:b2:79:1c:83:f4:07:00:cd:26:e4:
    c9:41:5d:4e:eb:78:de:7e:45:35:e0:a1:e3:03:71:
    25:3b:ab:96:43:fa:ba:08:ee:5a:9b:2c:8e:6a:9b:
    59:ca:94:d7:3e:ed:0b:18:c6:33:ed:8f:fe:dc:14:
    1e:84:6f:22:b8:58:04:93:30:60:2a:54:4f:12:05:
    be:21:86:65:a8:86:b8:54:10:26:5f:4c:af:74:db:
    41:d1:64:6a:03:22:de:77:ed:91:15:c9:0a:ee:29:
    b5:9a:89:33:ec:7b:4a:f3:31:90:fb:09:8a:f1:34:
    17:c0:6f:16:18:ce:45:5c:e5:c4:40:78:1d:91:64:
    ea:42:63:b8:8c:e9:dc:f1:82:72:39:13:8c:7e:1b:
    68:c6:62:fa:6d:a3:be:62:77:2e:70:1f:0d:f6:28:
    68:3b:50:d6:65:92:da:a3:aa:9b:54:f0:19:b8:cb:
    95:d1:2a:e2:c9:cd:76:cd:77:7f:0f:ee:0b:e4:8a:
    cb:03:4f:0e:27:45:32:b8:20:b8:36:63:9c:05:5e:
    b6
```

```
P:
    00:9c:c7:85:8c:59:00:f4:7b:44:a7:d9:07:0a:b7:
    fd:e8:84:56:24:4e:4d:ff:a8:12:9d:1a:ea:2a:a7:
    17:8b:72:f7:97:c1:65:5d:8d:5c:a6:de:8f:23:4e:
    f2:de:cb:f6:7e:27:d0:a8:e6:5c:77:f8:0f:d1:9d:
    fd:80:64:d4:99:da:cb:ba:0d:03:6a:9b:70:6b:a0:
    a6:a1:57:eb:d0:58:57:d8:74:5a:9e:de:66:80:39:
    94:40:da:83:94:8f:bd:14:fb:b0:75:78:cd:b0:18:
    91:b1:d7:7c:c9:d1:3a:20:34:0d:dc:ca:a5:31:f1:
    aa:b6:f0:57:be:9e:34:56:29:0d:04:22:b1:2b:4e:
    0f:60:3c:8e:32:c2:ea:93:81:11:ff:4b:fc:e6:dd:
    39:07:53:5a:5e:e1:2f:cc:89:24:98:52:88:8a:33:
    a5:fb:bf:71:56:12:c8:14:99:32:5c:13:c0:50:7d:
    b6:df:52:e5:bf:ef:f9:68:74:63:d3:28:a8:d2:ff:
    67:3e:1f:49:41:79:84:19:a3:e1:5c:54:f8:ed:12:
    d6:ca:32:30:54:96:2d:54:3b:55:b7:c8:56:8a:08:
    32:30:7c:02:7d:50:a1:a0:40:8d:b2:07:1c:ab:87:
    ff:ec:14:c6:be:ce:d0:71:fc:3d:49:fa:ca:cf:52:
    46:33
Q:
    00:e8:f0:eb:d2:45:b8:6d:39:49:65:da:7d:6f:97:
    f3:4f:4d:8d:72:84:dc:2b:ef:e0:66:04:de:1a:82:
    ec:c7:75
G:
    00:85:fc:38:2c:13:24:4d:69:78:12:01:3c:1d:16:
    b6:e9:5c:64:98:a3:06:8b:d0:a5:04:23:70:f7:bb:
    d7:d7:46:30:37:37:d5:50:86:44:15:04:e3:7e:bd:
    29:dc:a5:6e:fa:0d:ce:1b:8d:5b:8e:85:03:cc:3a:
    6c:a6:41:2d:b1:13:16:85:71:46:52:43:2e:84:1e:
    0a:7f:96:24:6d:cb:a9:32:f0:38:69:ad:46:aa:95:
    5f:97:60:e9:9f:9e:eb:e1:41:5d:c7:82:4f:1b:55:
    10:f8:2b:e5:2f:0c:4c:bb:99:f7:83:ff:fa:f6:cb:
    5f:55:bc:21:3b:84:78:ef:eb:31:5e:ee:be:00:48:
    eb:eb:a3:32:f0:b8:07:d1:0d:25:75:e3:8e:e1:b6:
    1d:7a:09:a3:4f:20:c2:68:9d:16:eb:d5:05:c7:a5:
    47:b6:56:51:6a:d7:e9:0c:35:e5:88:b8:94:89:ab:
    07:b3:2e:a0:f3:a9:77:91:bd:a3:83:ce:95:b9:ed:
    48:98:14:a3:3e:61:5a:4b:91:35:26:05:21:ba:4f:
    0c:a2:80:20:7a:ed:7d:92:a7:a6:9f:88:a5:1a:00:
    37:9f:66:9b:20:00:a4:c0:16:a1:3e:33:82:40:2e:
    e4:c4:46:61:90:e0:0e:37:79:c3:a3:de:3c:04:22:
    a7:52
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in cabreraDSAkey.pem -pubout -out cabreraDSApub.pem
read DSA key
writing DSA key
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in cabreraDSApub.pem -text -noout -pubin
read DSA key
pub:
    6f:f0:5a:60:32:ff:62:76:32:e0:eb:09:e3:dc:7a:
    2c:52:b4:56:52:af:02:47:d5:2c:ef:58:a3:97:d7:
    be:9a:2e:08:e3:91:00:b7:f6:fa:b2:d7:aa:d8:6c:
    05:27:84:b7:4a:97:eb:39:24:f8:de:00:a5:41:f3:
    7e:1d:25:4a:b4:77:0c:01:04:42:5d:67:a1:7e:88:
    98:3c:b9:b9:61:25:20:c9:2a:7c:04:f7:1a:b5:31:
    69:f9:6d:e0:d7:7b:f0:fe:8a:37:54:1e:0b:d5:41:
    ea:7d:b6:55:1f:cc:9e:ec:fd:02:0a:31:26:8d:5d:
    c4:04:b6:a9:cb:33:04:b3:e0:ab:31:5b:e2:80:23:
    50:7c:f4:60:e6:11:3b:37:2a:4f:49:4b:53:3d:6b:
    33:38:fe:64:3b:c5:5b:b0:a3:fb:d5:08:25:cf:21:
    36:96:fe:bd:20:0b:79:be:03:93:c4:14:f5:f0:bc:
    97:98:3b:40:08:c5:a4:55:cb:40:1d:1b:0e:4c:a2:
    4e:99:d6:1b:73:7a:91:eb:e2:fe:39:40:1b:f4:ff:
    42:d5:38:01:6e:c7:d4:ae:42:86:de:a5:51:fc:90:
    e0:26:3d:00:7c:14:a9:3a:c6:e4:89:71:5e:e8:48:
    ca:73:95:b3:4f:9d:0d:55:19:84:0a:c6:6b:8e:08:
    70
P:
    00:9c:c7:85:8c:59:00:f4:7b:44:a7:d9:07:0a:b7:
    fd:e8:84:56:24:4e:4d:ff:a8:12:9d:1a:ea:2a:a7:
    17:8b:72:f7:97:c1:65:5d:8d:5c:a6:de:8f:23:4e:
    f2:de:cb:f6:7e:27:d0:a8:e6:5c:77:f8:0f:d1:9d:
    fd:80:64:d4:99:da:cb:ba:0d:03:6a:9b:70:6b:a0:
    a6:a1:57:eb:d0:58:57:d8:74:5a:9e:de:66:80:39:
    94:40:da:83:94:8f:bd:14:fb:b0:75:78:cd:b0:18:
    91:b1:d7:7c:c9:d1:3a:20:34:0d:dc:ca:a5:31:f1:
    aa:b6:f0:57:be:9e:34:56:29:0d:04:22:b1:2b:4e:
    0f:60:3c:8e:32:c2:ea:93:81:11:ff:4b:fc:e6:dd:
    39:07:53:5a:5e:e1:2f:cc:89:24:98:52:88:8a:33:
    a5:fb:bf:71:56:12:c8:14:99:32:5c:13:c0:50:7d:
    b6:df:52:e5:bf:ef:f9:68:74:63:d3:28:a8:d2:ff:
    67:3e:1f:49:41:79:84:19:a3:e1:5c:54:f8:ed:12:
    d6:ca:32:30:54:96:2d:54:3b:55:b7:c8:56:8a:08:
    32:30:7c:02:7d:50:a1:a0:40:8d:b2:07:1c:ab:87:
    ff:ec:14:c6:be:ce:d0:71:fc:3d:49:fa:ca:cf:52:
    46:33
Q:
    00:e8:f0:eb:d2:45:b8:6d:39:49:65:da:7d:6f:97:
    f3:4f:4d:8d:72:84:dc:2b:ef:e0:66:04:de:1a:82:
    ec:c7:75
```

```
G:
    00:85:fc:38:2c:13:24:4d:69:78:12:01:3c:1d:16:
    b6:e9:5c:64:98:a3:06:8b:d0:a5:04:23:70:f7:bb:
    d7:d7:46:30:37:37:d5:50:86:44:15:04:e3:7e:bd:
    29:dc:a5:6e:fa:0d:ce:1b:8d:5b:8e:85:03:cc:3a:
    6c:a6:41:2d:b1:13:16:85:71:46:52:43:2e:84:1e:
    0a:7f:96:24:6d:cb:a9:32:f0:38:69:ad:46:aa:95:
    5f:97:60:e9:9f:9e:eb:e1:41:5d:c7:82:4f:1b:55:
    10:f8:2b:e5:2f:0c:4c:bb:99:f7:83:ff:fa:f6:cb:
    5f:55:bc:21:3b:84:78:ef:eb:31:5e:ee:be:00:48:
    eb:eb:a3:32:f0:b8:07:d1:0d:25:75:e3:8e:e1:b6:
    1d:7a:09:a3:4f:20:c2:68:9d:16:eb:d5:05:c7:a5:
    47:b6:56:51:6a:d7:e9:0c:35:e5:88:b8:94:89:ab:
    07:b3:2e:a0:f3:a9:77:91:bd:a3:83:ce:95:b9:ed:
    48:98:14:a3:3e:61:5a:4b:91:35:26:05:21:ba:4f:
    0c:a2:80:20:7a:ed:7d:92:a7:a6:9f:88:a5:1a:00:
    37:9f:66:9b:20:00:a4:c0:16:a1:3e:33:82:40:2e:
    e4:c4:46:61:90:e0:0e:37:79:c3:a3:de:3c:04:22:
    a7:52
```

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

Archivo elegido message.txt

6. (0,5 puntos) 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.

```
mati@mati-VirtualBox:~/Escritorio/Practica3$ openssl pkeyutl -sign -in
message.txt -inkey matiDSApriv.pem -out message.sign
Enter pass phrase for matiDSApriv.pem:
```

```
mati@mati-VirtualBox:~/Escritorio/Practica3$ openssl dsa -in message.si
gn -text -noout
read DSA key
unable to load Private Key
139689734342336:error:0906D06C:PEM routines:PEM_read_bio:no start line:
pem_lib.c:696:Expecting: ANY PRIVATE KEY
unable to load Key
mati@mati-VirtualBox:~/Escritorio/Practica3$ sudo cat message.sign
[illegible]Iy''vt[illegible]mati@mati-VirtualBox:~/Escritorio/Practica3$
```

```
xxd message.sign
00000000: 3046 0221 00c3 26df 69d5 2667 6c7f 121b  0F.!..&.i.&gl...
00000010: 7170 86ba be3c 75b1 f977 fff7 6635 e9af  qp...<u..w..f5..
00000020: 497e 1384 bf02 2100 e860 38ae da05 74bf  I~....!..`8...t.
00000030: eecd 0d36 837b e8bd 2c99 27f5 4dc7 5414  ...6.{..,.'.M.T.
00000040: 87ff 0ec5 241b 0b5a                      ....$..Z
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

7. (1 punto) Construid un archivo message2 diferente de message tal que la verificación de la firma message.sign sea correcta con respecto al archivo message2 .

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
ssl pkeyutl -verify -in message2 -sigfile message.sign -inkey matiDSApriv.pem
Enter pass phrase for matiDSApriv.pem:
Signature Verified Successfully
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ cat
message.txt
{
    "mati331@correo.ugr.es":[{
                "user" : "mati",
                "ape" : "cabrera",
                "edad" : "40",
                "email": "mati331@correo.ugr.es",
                "telef" : "637423567",
                "passwd": "1234"
               }
        ]
}
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ cat
message2
{
    "mati331@correo.ugr.es":[{
                "user" : "mati",
                "ape" : "cabrera",
                "edad" : "40",
                "email": "mati331@correo.ugr.es",
                "telef" : "637423567",
                "passwd": "1234"
               }
        ]
}
y pongo algo mas que en message.txt
```

8. (0,5 puntos) Calculad el valor hash del archivo con la clave publica 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.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
ssl dgst -sha384 -hex -out matiDSApub.sha384  matiDSApub.pem
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ cat
matiDSApub.sha384
SHA384(matiDSApub.pem)= 45b4e8d3653760656497cf735f2fd633709e137c4728117c422c0758
846c163d3df31e0e81247ab056afd824b027cd4d
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
ssl dgst -sha384 -hex -out matiDSApub.sha384 -c matiDSApub.pem
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ cat
matiDSApub.sha384
SHA384(matiDSApub.pem)= 45:b4:e8:d3:65:37:60:65:64:97:cf:73:5f:2f:d6:33:70:9e:13
:7c:47:28:11:7c:42:2c:07:58:84:6c:16:3d:3d:f3:1e:0e:81:24:7a:b0:56:af:d8:24:b0:2
7:cd:4d
```

9. (0,5 puntos) Calculad el valor hash de message2 usando una función hash de 160 bits con salida binaria. Guardad el hash en message2.<algoritmo> y mostrad su contenido.

```
ati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
sl dgst -sha1 -binary -out message2.sha1 message2
ati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ xxd
essage2.sha1
0000000: 9a3e c885 c1bf 08e7 f03a 3aab 8d9b 728f  .>.......:...r.
0000010: d07f 091f                                ....
ati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

10. (0,5 puntos) 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.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dgst -sha1 -sign matiDSApriv.pem -out message2.sign message2
Enter pass phrase for matiDSApriv.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dsa -in message2.sign -text -noout
read DSA key
unable to load Private Key
140708664596160:error:0906D06C:PEM routines:PEM_read_bio:no start line:pem_l
ib.c:696:Expecting: ANY PRIVATE KEY
unable to load Key
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
xxd message2.sign
00000000: 3046 0221 0082 2241 fa4b 22e3 9eeb 9b05  0F.!.."A.K".....
00000010: 2686 a6a1 abe2 30ad ce62 b640 9dc8 c8b9  &.....0..b.@....
00000020: 2e16 3fe0 a802 2100 89d7 a1f2 1450 a313  ..?...!......P..
00000030: 68f3 9085 12d0 681f c920 3c0d 27cb 7951  h.....h.. <.'.yQ
00000040: 9673 1447 18e2 4554                      .s.G..ET
```

11. (1 punto) Verificad la firma message2.sign con los archivos message y message2 empleando el comando openssl dgst.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dgst -sha1 -verify matiDSApub.pem -signature message2.sign message2
Verified OK
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
ssl dgst -sha1 -verify matiDSApub.pem -signature message2.sign message.txt
Verification Failure
```

Message2 lo verifica sin problema, message.txt como es evidente, al usar la función hash, no lo puede verificar.

12. (0,5 puntos) Verificad que message2.sign es una firma correcta para message2 pero empleando el comando openssl pkeyutl

Me da error porque tengo que usar el hash de message2 calculado antes en binario, en el ejercicio 9.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ open
ssl pkeyutl -verify -in message2 -sigfile message2.sign -inkey matiDSApriv.pem
Enter pass phrase for matiDSApriv.pem:
Signature Verification Failure
```

Como podemos ver ahora si:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ openssl p
keyutl -verify -in message2.sha1 -sigfile message2.sign -pubin -inkey matiDSApub.pem
Signature Verified Successfully
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

13. (0,5 puntos) Generad el valor HMAC del archivo sharedDSA.pem con clave ’12345’ mostrándolo por pantalla.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
openssl dgst -hmac 12345 sharedDSA.pem
HMAC-SHA1(sharedDSA.pem)= 50b7e2230cfb17bf137b8dde7b8df3ba5a416e22
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$
```

14. (3 puntos) Simulad una ejecución completa del protocolo Estación a Estación. Para ello emplearemos como claves para firma/verificacion las generadas en esta practica, y para el protocolo DH emplearemos las claves asociadas a curvas elípticas de la practica anterior junto con las de otro usuario simulado que deberéis generar nuevamente. Por

ejemplo, si mi clave privada está en javierECpriv.pem y la clave publica del otro usuario está en lobilloECpub.pem , el comando para generar la clave derivada será

$> openssl pkeyutl -inkey javierECpriv.pem -peerkey lobilloECpub.pem -derive -out key.bin

El algoritmo simétrico a utilizar en el protocolo estación a estación será AES-128 en modo CFB8 .

Traigo de la practica anterior:
matiECpriv.pem
matiECpub.pem
stdECparam.pem

Creo dos nuevas carpetas (mati y cabrera) y guardo cada archivo en su carpeta correspondiente simulando así dos usuarios, mati tendrá los archivos de la practica anterior.

Usuario cabrera (a partir de stdECparam.pem generamos cabreraECpub.pem y cabreraECpriv.pem).

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ openssl
 ecparam -in stdECparam.pem -genkey -out cabreraECkey.pem
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ openssl
 ec -in cabreraECkey.pem -aes128 -out cabreraECpriv.pem
read EC key
writing EC key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3$ openssl
 ec -in cabreraECkey.pem -pubout -out cabreraECpub.pem
read EC key
writing EC key
```

Punto de partida de las carpetas:

mati:
- matiECpriv.pem
- matiECpub.pem
- matiDSApriv.pem
- matiDSApub.pem
- cabreraDSApub.pem

cabrera:
- cabreraECpriv.pem
- cabreraECpub.pem
- cabreraDSApriv.pem
- cabreraDSApub.pem
- matiDSApub.pem

Todas las contraseñas son “0123456789”

Primer usuario mati manda al usuario cabrera el archivo matiECpub.pem
Usuario cabrera genera la clave derivada con su clave privada EC y la clave publica EC de mati:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 openssl pkeyutl -derive -inkey cabreraECpriv.pem -peerkey matiECpub.pem -out cabre
raDerive.bin
Enter pass phrase for cabreraECpriv.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 xxd cabreraDerive.bin
00000000: 052b b216 4ab2 1a03 de81 4afe 4f1d 238c  .+..J.....J.O.#.
00000010: ed64 0cd8 d4                             .d...
```

Usuario cabrera concatena su clave publica junto con la de usuario mati:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabre
ra$ cat matiECpub.pem cabreraECpub.pem > concatenaCabrera
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabre
ra$ cat concatenaCabrera
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAA8DLAAEApYMcQUptTVOl4sQdYGRzb4RROKzAOzp
0t+0FPvXb7e32NoeCBoE2RPx
-----END PUBLIC KEY-----
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAA8DLAAEBEqCLDDsytQpHq/k4fX+sj27g7ZLAFyA
M5qUxWaoSCUVOWZFsxwqdY6X
-----END PUBLIC KEY-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabre
```

Usuario cabrera firma con su clave privada el archivo anterior “concatenaCabrera” y lo cifra con aes-128-cfb8, resultado en firmaConcatCabreraCifrado:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 openssl dgst -sign cabreraDSApriv.pem -out firmaConcatCabrera concatenaCabrera
Enter pass phrase for cabreraDSApriv.pem:
[00m$ i-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 openssl enc -aes-128-cfb8 -in firmaConcatCabrera -out firmaConcatCabreraCifrado -p
ass file:cabreraDerive.bin
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 xxd firmaConcatCabrera
00000000: 3043 0220 60fd ac81 4d3d 5891 ac9d 4623  0C. `...M=X...F#
00000010: b200 000f e523 a96e 7c55 37c6 fd20 a7dd  .....#.n|U7.. ..
00000020: 8402 9f3d 021f 2fe7 3219 93f1 1be6 17f0  ...=../.2.......
00000030: 6292 13b7 e2d2 f109 a3a6 bf36 3fc5 b4aa  b..........6?...
00000040: 9c05 19f9 f3                             .....
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
 xxd firmaConcatCabreraCifrado
00000000: 5361 6c74 6564 5f5f 706c 5a03 6d69 0a4e  Salted__plZ.mi.N
00000010: ad49 974c c4ff 7973 9866 df3b 557c 88d6  .I.L..ys.f.;U|..
00000020: 9958 37df 96d4 bd14 587f e2b9 419c 87a7  .X7.....X...A...
00000030: 5289 af3c f2b1 e861 961a 95b9 cfdc bb11  R..<...a........
00000040: 1929 0973 dbf8 7a8c 6678 b053 54ae 4507  .).s..z.fx.ST.E.
00000050: 4aa7 94cc 98                             J....
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/cabrera$
```

Usuario cabrera manda a usuario mati el archivo cabreraECpub.pem junto con el archivo firmaConcatCabreraCifrado (concatenacion de claves publicas firmada y cifrada por cabrera).

Usuario mati recibe los archivos, primero genera la clave derivada con su clave privada EC y la clave publica EC de cabrera:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$ op
enssl pkeyutl -derive -inkey matiECpriv.pem -peerkey cabreraECpub.pem -out matiDeri
ve.bin
Enter pass phrase for matiECpriv.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$ xx
d matiDerive.bin
00000000: 052b b216 4ab2 1a03 de81 4afe 4f1d 238c  .+..J.....J.O.#.
00000010: ed64 0cd8 d4                             .d...
```

Usuario mati descifra el archivo firmaConcatCabreraCifrado. Salida en firmaConcatCabreraDescifrado.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$ op
enssl enc -aes-128-cfb8 -d -in firmaConcatCabreraCifrado -out firmaConcatCabreraDes
cifrado -pass file:matiDerive.bin
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$ xx
d firmaConcatCabreraDescifrado
00000000: 3045 0221 00b0 db49 8ebf 12eb 6488 1ef2  0E.!...I....d...
00000010: af1b 3bed b78e e3a9 c5d4 4841 0c58 4d71  ..;.......HA.XMq
00000020: 85f0 1123 4802 2018 a930 e0d1 f623 8980  ...#H. ..0...#..
00000030: e710 ff25 1db9 398e 1d8a 2322 cadd bb3b  ...%..9...#"...;
00000040: ad6c 488f 52eb cc                        .lH.R..
```

Usuario mati concatena las claves públicas de matiECpub.pem y cabreraECpub.pem (al contrario para poder verificar el archivo de cabrera, asi que lo hace como si fuera cabrera). Luego verifica el archivo anterior descifrado “firmaConcatCabreraDescifrado” con la concatenación.

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
cat matiECpub.pem cabreraECpub.pem > concatenaCabrera2
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
openssl dgst -verify cabreraDSApub.pem -signature firmaConcatCabreraDescifrado co
ncatenaCabrera2
Verified OK
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
```

Ahora usuario mati va a realizar el mismo proceso, genera su clave derivada, concatena las claves publicas, firma, cifra y manda a cabrera esperando que este pueda descifrar y verificar.

Usuario mati genera la clave derivada con su clave privada EC y la clave publica EC de cabrera:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
openssl pkeyutl -derive -inkey matiECpriv.pem -peerkey cabreraECpub.pem -out mati
Derive.bin
Enter pass phrase for matiECpriv.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
xxd matiDerive.bin
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
xxd matiDerive.bin
00000000: 052b b216 4ab2 1a03 de81 4afe 4f1d 238c  .+..J.....J.O.#.
00000010: ed64 0cd8 d4                             .d...
```

Usuario mati concatena su clave publica junto con la de usuario cabrera:

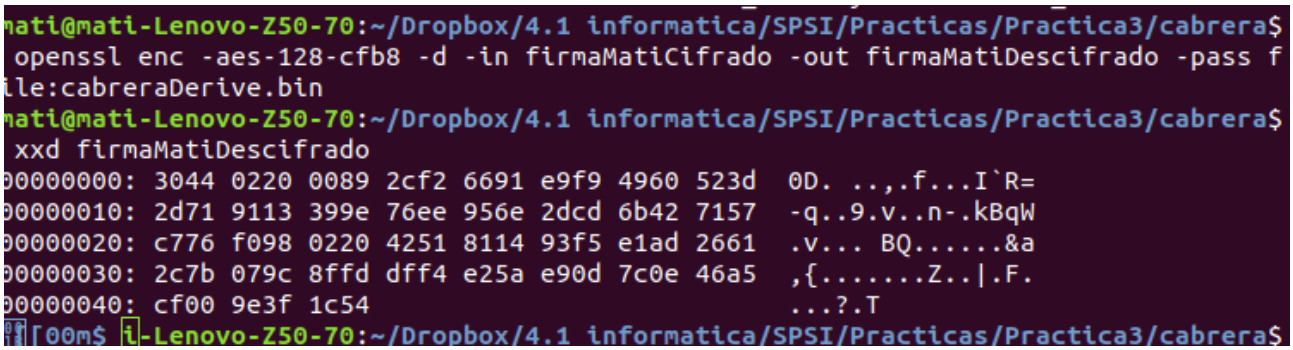
```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
cat cabreraECpub.pem matiECpub.pem >concatenaMati
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
cat concatenaMati
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAA8DLAAEBEqCLDDsytQpHq/k4fX+sj27g7ZLAFyA
M5qUxWaoSCUVOWZFsxwqdY6X
-----END PUBLIC KEY-----
-----BEGIN PUBLIC KEY-----
MEAwEAYHKoZIzj0CAQYFK4EEAA8DLAAEApYMcQUptTVOl4sQdYGRzb4RROKzAOzp
0t+0FPvXb7e32NoeCBoE2RPx
-----END PUBLIC KEY-----
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
```

Usuario mati firma con su clave privada el archivo anterior “concatenaMatiCabrera” y lo cifra con aes-128-cfb8, resultado en firmaConcatMatiCifrado:

```
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
openssl dgst -sign matiDSApriv.pem -out firmaMati concatenaMati
Enter pass phrase for matiDSApriv.pem:
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
openssl enc -aes-128-cfb8 -in firmaMati -out firmaMatiCifrado -pass file:matiDeri
ve.bin
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
xxd firmaMatiCifrado
00000000: 5361 6c74 6564 5f5f 643b 27ef 8ab4 8b9e  Salted__d;'.....
00000010: 398f 88a2 804d c9af bda8 e771 562d 665e  9....M.....qV-f^
00000020: 29ef 6b26 b55a 129b 2660 5b55 1915 4686  ).k&.Z..&`[U..F.
00000030: 2be7 da2f 7b38 ce8d 2b2b 67b9 493b 68ff  +../{8..++g.I;h.
00000040: 6792 1adc 1a32 4c47 2303 9aea 8003 0a81  g....2LG#.......
00000050: 26ae c0fc 577f                           &...W.
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
xxd firmaMati
00000000: 3044 0220 0089 2cf2 6691 e9f9 4960 523d  0D. ..,.f...I`R=
00000010: 2d71 9113 399e 76ee 956e 2dcd 6b42 7157  -q..9.v..n-.kBqW
00000020: c776 f098 0220 4251 8114 93f5 e1ad 2661  .v... BQ......&a
00000030: 2c7b 079c 8ffd dff4 e25a e90d 7c0e 46a5  ,{.......Z..|.F.
00000040: cf00 9e3f 1c54                           ...?.T
mati@mati-Lenovo-Z50-70:~/Dropbox/4.1 informatica/SPSI/Practicas/Practica3/mati$
```

Usuario mati manda a usuario mati el archivo firmaMatiCifrado (concatenacion de claves publicas firmada y cifrada por mati).

Usuario cabrera recibe el archivos, ya tiene la clave derivada, es cabreraDerive.bin. Descifra el archivo firmaMati. Salida en firmaMatiDescifrado. Como podemos ver en la imagen anterior el archivo descifrado es igual a “firmaMati”



Usuario cabrera concatena las claves públicas de cabrera ECpub.pem y matiECpub.pem (al contrario para poder verificar el archivo de mati, asi que lo hace como si fuera mati). Luego verifica el archivo anterior descifrado “firmaMatiDescifrado” con la concatenación.