Escuela Superior
de Ingeniería y Tecnología
Universidad de La Laguna

Práctica 04. Confidencialidad con clave pública en OpenSSL

Seguridad de Sistemas Informáticos

Cheuk Kelly Ng Pante
alu0101364544@ull.edu.es

1. Generar un certificado personal con getaCert **2**
2. Extrayendo información de un certificado con OpenSSL **3**
2.1. Convertimos al formato PEM el fichero que contiene su certificado 3
2.2. Muestra en la consola la clave pública contenida en tu certificado. 4
2.3. Extrae la clave pública del certificado y la clave privada del certificado cifrándola con triple des 5
2.4. Firma con la clave privada asociada al certificado generado el fichero DancingMan.txt 6
2.5. Verifica la firma que acabas de generar 6

1. Generar un certificado personal con getaCert

getaCert

Review your self-signed certificate

Please review your certificate details carefully before submitting it.

Self-signed certificate details	
Hostname or your full name	Cheuk Kelly Ng Pante
Organisation/Company	ULL
Email	srchaki10@gmail.com
City/Local	La Laguna
State	Santa Cruz de Tenerife
Country	ES
Expiration	1

Your self-signed certificate page :

Private key : Cheuk-2023-10-13-074140.pkey

Open Private key

Certificate request (.csr) : Cheuk-2023-10-13-074140.csr

Open Certificate request (.csr)

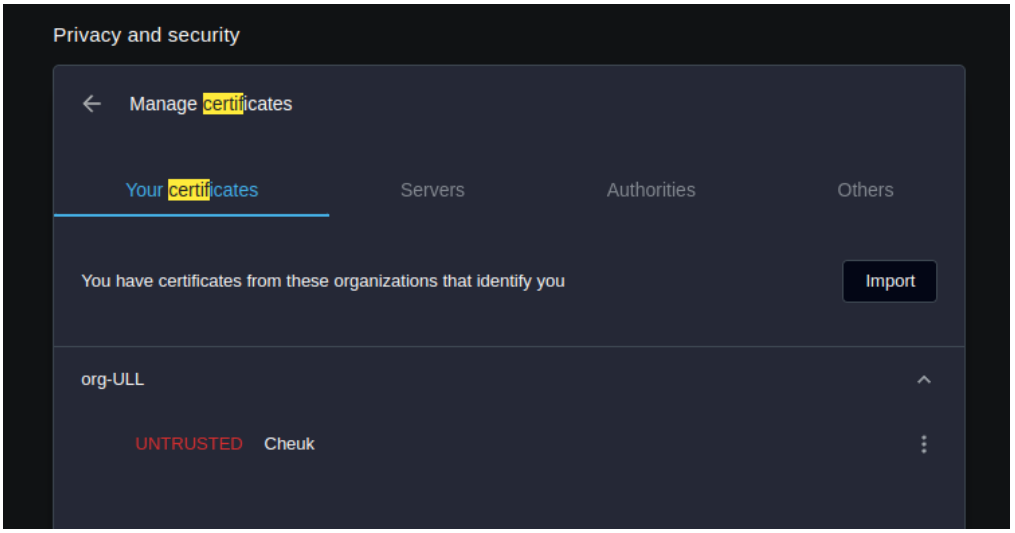
Public key(.cer) : Cheuk-2023-10-13-074140.cer

Open Public key(.cer)

Entire certificate (pkcs12) : Cheuk-2023-10-13-074140.p12

Note: Your certificate password is the word 'password' (without any quote marks)

About Us | Privacy Statement | Home



2. Extrayendo información de un certificado con OpenSSL

2.1. Convertimos al formato PEM el fichero que contiene su certificado

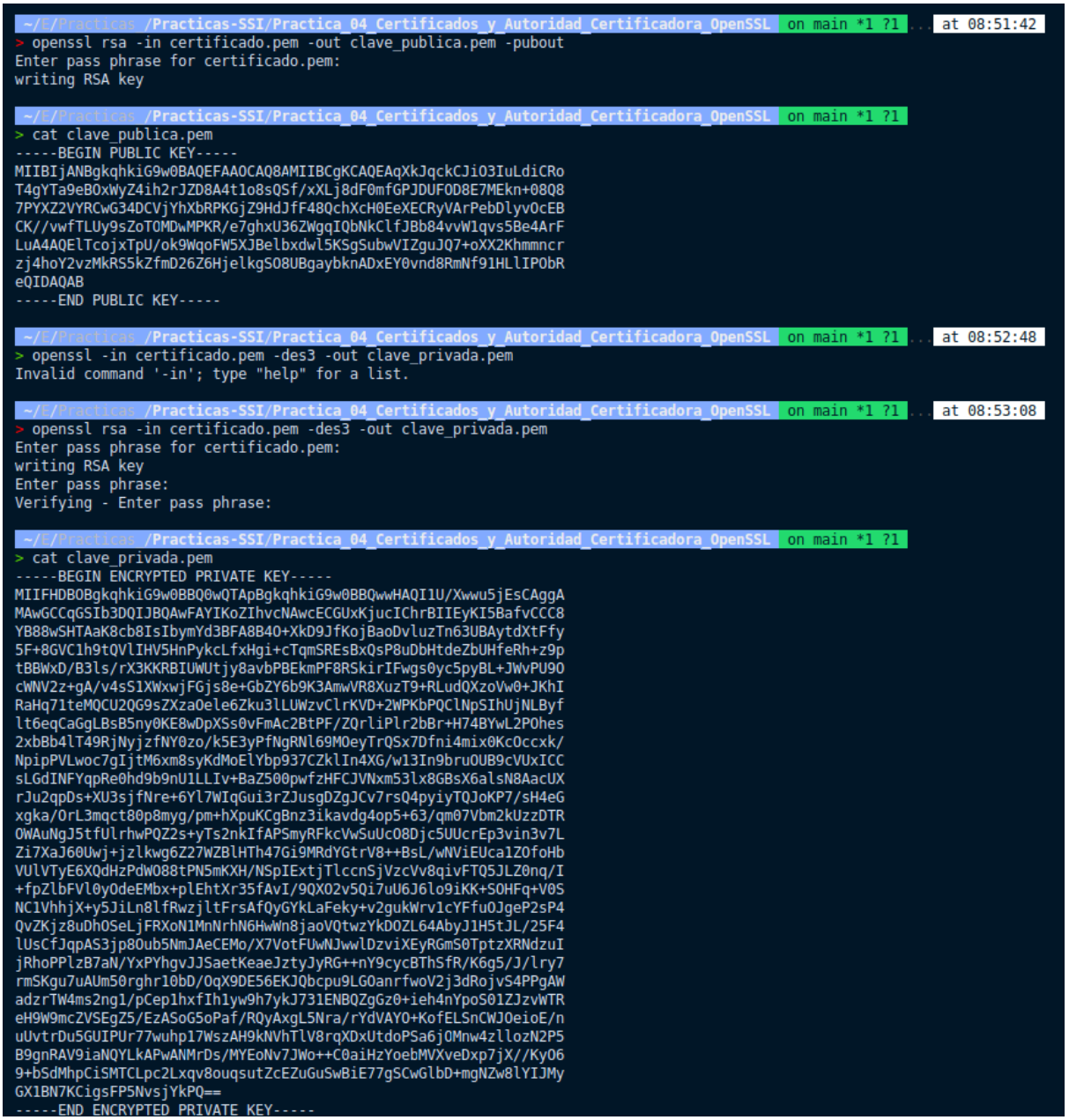
```
~/E/Practicas-SSI/Practica_04_Certificados_y_Autoridad_Certificadora_OpenSSL on main *1 ?1
> openssl pkcs12 -in Cheuk-2023-10-13-074140.p12 -out certificado.pem -clcerts -legacy
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
/mnt/d/D/I/4/P/Sc/Practicas-SSI/Practica_04_y_05_Certificados_y_Autoridad_Certificadora_OpenSSL on
main !1 ?2
└─ cat certificado.pem
Bag Attributes
    friendlyName: Cheuk
    localKeyID: 83 51 C4 09 47 DA A7 CD E1 79 21 59 B5 6B 83 2F 6E DE BA C8
subject=C = ES, ST = Canarias, L = La Laguna, O = ULL, CN = Cheuk, emailAddress = alu0101364544@ull.edu.es
issuer=C = ES, ST = Canarias, L = La Laguna, O = ULL, CN = Cheuk, emailAddress = alu0101364544@ull.edu.es
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIUBsMgaGfGQtxTEpFUmncwwvQX7I0wDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRVMxETAPBgNVBAgTCENhbmFyaWFzMRIwEAYDVQQHEwlM
YSBMYWd1bmExDDAKBgNVBAoTA1VMTDEQMAwGA1UEAxMFQ2hldWsxJzAlBgkqhkiG
9w0BCQEWGGFsdTAxMDEzNjQ1NDRAdWxsLmVkdS51czAeFw0yMzEwMTMwNzQxNDBa
Fw0yMzEwMTQwNzQxNDBaMHsxCzAJBgNVBAYTAkVTMREwDwYDVQQIEwhDYW5hcmlh
czESMBAGA1UEBxMJTGEgTGFndW5hMQwwCgYDVQQKEwNVTEwxDjAMBgNVBAMTBUNo
ZXVrMScwJQYJKoZIhvcNAQkBFhhhbHUwMTAxMzY0NTQ0QHVsbC51ZHUuZXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpeQmpyQImI7ci4t2IJGhPiBhN
r14E7FbJniKHaslkPwDi3WjyxBJ//FcuPx0XSZ8Y8kNQU4PwTswSSf7TxDzs9hdn
ZVhELAbfgMJWNiFdtE8oaNn0d0l8XjxByFdwfQR5cQJHJUCs95sOXK85wQEIr/+/
B9MtTL2xmhM4wPAw8pH97uCHFTfplaCohBs2QkV8kFvzi+9bWq+zkF7gCsUu4DgB
ASVNyiPFOlT+iT1aqgVblckF6VvF3CXkpKBK5vBUhmC41Dv6hdfYqGaadyvOPiGh
ja/MyRFLmRl+YPbpnoeN6WSBI7xQGBrJuScAPERjS+d3xGY1/3UcuUg85tF5AgMB
AAGjTDBKMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgTwMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQAD
ggEBAIYJ7qgUb9QcTSHWTnhIADd31Fy0KuGnq6LwWvEAtA82FTiA44KHW/chAsG5
mPS9ndcusTEG8wfzcX/gDdLt/sbneUKH3OHeu/569uXGtiK1XJvzaMY0i4jnCsHa
XTueOHfvhMvVQPTCY2z1ExmssFt8pG3DBSXIZ91J+sVu87Ob4q3EYElczA7vpeei
pySvOd8ejt/76dioVhzFG+qapYVD9IeI1Vma/N3TiOci3d2+8r56LI3r58aUK5wD
mbLq29oEPJX2z3a6PGziRVCSUqvNURsqV4h3z2/H/sLp6q08YJQJRZyeu2K18N1z
Yl6rnGxag1bsItaj2otwPPn3Zxg=
-----END CERTIFICATE-----
Bag Attributes
    friendlyName: Cheuk
    localKeyID: 83 51 C4 09 47 DA A7 CD E1 79 21 59 B5 6B 83 2F 6E DE BA C8
Key Attributes: <No Attributes>
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIYp2wUJ0x348CAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECIZHPoHPr3oGBIIEyMhodxoEnrpi
kj/119poyFgKYgvrgtvdQhmI084mktn5tqKahnDG4Xz3SgrrJ512hK2py5WNed86
T4jkotLUgoCH2yuy7hWrVKekC3IoI8jH9bgocNH2xG01zSScaeWdh/0OpTeIT0Um
UDAPmmMIXKZIRPHkZFEwjb+ijoFBAT5/Obg+2fKIgyxu0IWyKR8E+Dmb3+d3cGFx
5aWFLF5kuFMGLfPCRbLGNR5Hc3xX3y2FBTup0EExIvVvBqk47b4arXZ6e1Jei1B9
xV9QjUkyeh27CIW8A7FNF/3pGldvFuIGX3XjckRkmeKt2B1M2FNnT5hayCVcp9Fs
3cYkxaVRPVf0sxShnYIJsVBDbhIoWuH1TPNudbF8q/DlCxEJkQ8TA0XhF35T5TzY
claXboA2YgQPvHS0UWR8AI7TI0nawQuF37sSEziI8tIZnfZtK3f4P6wEkVOZdHYF
cz6vaS2hIayVQQ8M2AimAYPkODEMDTQpZsr4kBLGbD0ODzU7aJQQhrIHxK2sFcU4
eeiHTTWvPyPhkdpiPHB2zwBqMJMpiJ5PTyi4E4gz3g84HWJC5b9C21DB7uoSEoh1
1F35CnGpSr7PeJTE4tfxCEZAY5/yLOiQRSJhpW0oFtifQ5ZxQ0rR9q+s08mauPQc
mcxGxSmlEs+T6avAvVEjxzOsgYfjMGJ7eBtfoCfVw98sFZp4iXSDBXn0dLm/kC1s
itJFNH+01Xq+glKZ6P5AsmeqzOfj+19jNayRJEC1XYnAogJQEKROe9LUwXhBLrXJ
ellb7S4ahPLa70aYo4ymEZKpL9OYH/WBDyX+ILRHSrVSAiMZlvHQZuDh6OMqvPhp
br8wfbb8U+sqBblcIm88eMJM2fIU1BoBrkSAxd0vaI+VnkapzfORpLU937rgHFHP
ngas0tQ2BHDJ/obMukWHJ8UyioOwr4kAojuLcjxZrbhuUP1Tk/hMxMwA47nrFt9y
3/XoLv+2kmgYiPbhzQ8F1ozd4QfIdvmA4/YfFTyW6NbFdWhNqvs1Dex1I78BQk0m
7Dd+PLtoHW9uOcowIP6LByCfaRg7lZhXcpU9Hxp6gVz8uywBye57wHpInCD1YwAR
43GZkhp6clKhLbvRXG8PZ1jaYKa9fuxq7xw+1yzcaguRCJmUB1MNxJsojgSsLYaB
ukh3CyiK7Mkwc6coq54WDEQTeCebUQw7YVIpbylPbR53scAHLeqhbb+AKZpnsmno
AOxKVDVD3V+sn6mKix011NtzBS5IkH8yqRTU8tb0YjEIVqliYQxVbq0w18JYTH+e
U8F2YOBMSLvl3f4kLGuN69ReJjaDmCa9SZUJChvrTpC0M1NmgQkd/6yy8mEVuZsL
cTczN6l+syrrunCpclRod3RBkoF53Ky2j44PiVyaaEptdJCUVsvzkH1+pCOimVYy
Fcq6ovJjQE0L6LmSucbACRxQrkZNyB7AJt/p7RSztnMsSHyjJuM7G/DRAtUbD+3x
NVtP17UhPg/1fshz7Xpt4TLfkGBTrutggkK1h1l8b94ajs5xMhl4obpj6gcI5+yvk
8YEoul5s66/wCL2TiJX90ecpjRuBaeJ9DZgqB/Z+gCCC1qQ/oDKogmb/Ku2/jwLY
2DHtNhnIJjjFuisWdMl+3w==
-----END ENCRYPTED PRIVATE KEY-----
```

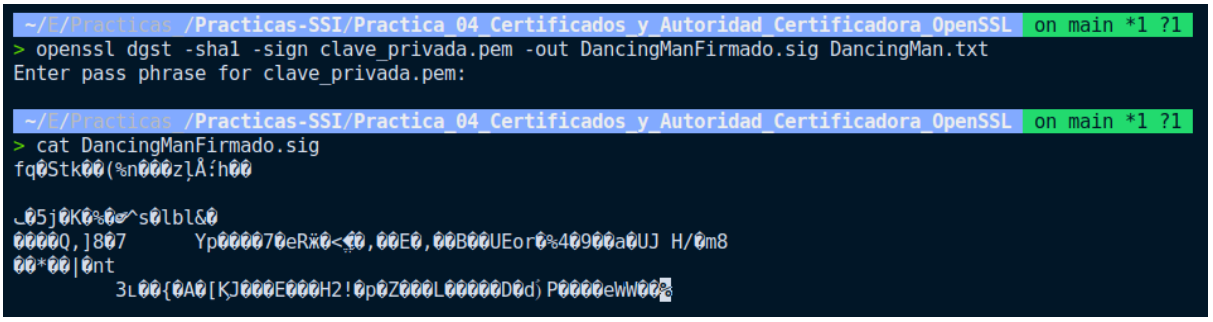
2.2. Muestra en la consola la clave pública contenida en tu certificado.

```
~/E/Practicas-SSI/Practica_04_Certificados_y_Autoridad_Certificadora_OpenSSL on main *1 ?1 .. at 00:50:46
> openssl x509 -text -in certificado.pem
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            06:c3:20:68:67:c6:42:dc:53:12:91:54:9a:77:30:c2:f4:17:ec:8d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = ES, ST = Canarias, L = La Laguna, O = ULL, CN = Cheuk, emailAddress = alu0101364544@ull.edu.es
        Validity
            Not Before: Oct 13 07:41:40 2023 GMT
            Not After : Oct 14 07:41:40 2023 GMT
        Subject: C = ES, ST = Canarias, L = La Laguna, O = ULL, CN = Cheuk, emailAddress = alu0101364544@ull.edu.es
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a9:79:09:a9:c9:02:26:23:b7:22:e2:dd:88:24:
                    68:4f:88:18:4d:af:5e:04:ec:56:c9:9e:22:87:6a:
                    c9:64:3f:00:e2:dd:68:f2:c4:12:7f:fc:57:2e:3f:
                    1d:17:49:9f:18:f2:43:50:53:83:f0:4e:cc:12:49:
                    fe:d3:c4:3c:ec:f6:17:67:65:58:44:2c:06:df:80:
                    c2:56:36:21:5d:b4:4f:28:68:d9:f4:77:49:7c:5e:
                    3c:41:c8:57:70:7d:04:79:71:02:47:25:40:ac:f7:
                    9b:0e:5c:af:39:c1:01:08:af:ff:bf:07:d3:2d:4c:
                    bd:b1:9a:13:38:c0:f0:30:f2:91:fd:ee:e0:87:15:
                    37:e9:95:a0:a8:84:1b:36:40:a5:7c:90:5b:f3:8b:
                    ef:5b:5a:af:b3:90:5e:e0:0a:c5:2e:e0:38:01:01:
                    25:4d:ca:23:c5:3a:54:fe:89:3d:5a:aa:05:5b:95:
                    c9:05:e9:5b:c5:dc:25:e4:a4:a0:4a:e6:f0:54:86:
                    60:b8:94:3b:fa:85:d7:d8:a8:66:9a:77:2b:ce:3e:
                    21:a1:8d:af:cc:c9:11:4b:99:19:7e:60:f6:e9:9e:
                    87:8d:e9:64:81:23:bc:50:18:1a:c9:b9:27:00:3c:
                    44:63:4b:e7:77:c4:66:35:ff:75:1c:b9:48:3c:e6:
                    d1:79
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, SSL Server, S/MIME, Object Signing
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        86:09:ee:a8:14:6f:d4:1c:4d:21:d6:4e:78:48:00:37:77:94:
        5c:b4:2a:e1:a7:ab:a2:f0:5a:f1:00:b4:0f:36:15:38:80:e3:
        82:87:5b:f7:21:02:c1:b9:98:f4:bd:9d:d7:2e:b1:31:06:f3:
        07:f3:71:7f:e0:0d:d2:ed:fe:c6:e7:79:42:87:dc:e1:de:bb:
        fe:7a:f6:e5:c6:b6:22:b5:5c:9b:f3:68:c6:34:8b:88:e7:0a:
        c1:da:5d:3b:9e:38:77:ef:84:cb:d5:40:f4:c2:63:6c:f5:13:
        19:ac:b0:5b:7c:a4:6d:c3:05:25:c8:67:d9:49:fa:c5:6e:f3:
        b3:9b:e2:ad:c4:60:49:5c:cc:0e:ef:a5:e7:a2:a7:24:af:39:
        df:1e:8e:df:fb:e9:d8:a8:56:1c:c5:1b:ea:9a:a5:85:43:f4:
        87:88:95:59:9a:fc:dd:d3:88:e7:22:dd:dd:be:f2:be:7a:2c:
        8d:eb:e7:c6:94:2b:9c:03:99:b2:ea:db:da:04:3c:95:f6:cf:
        76:ba:3c:6c:e2:45:50:92:52:ab:cd:51:1b:2a:57:88:77:cf:
        6f:c7:fe:c2:e9:ea:ad:3c:60:94:09:45:9c:9e:bb:62:a5:f0:
        dd:73:62:5e:ab:9c:6c:5a:83:56:ec:22:d6:a3:da:8b:70:3c:
        f9:f7:67:18
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIUBsMgaGfGQtxTEpFUmncwwvQX7I0wDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRVMxETAPBgNVBAgTCENhbmFyaWFzMRIwEAYDVQQHEwlM
YSBMYWd1bmExDDAKBgNVBAoTA1VMTDECMAwGA1UEAxMFQ2hldWsxJzAlBgkqhkiG
9w0BCQEWGGFsdTAxMDEzNjQ1NDRAdWxsLmVkd55lczAeFw0yMzEwMTMwNzQxNDBa
Fw0yMzEwMTQwNzQxNDBaMHsxCzAJBgNVBAYTAkVTMREwDwYDVQQIEwhDYW5hcmlh
czESMBAGA1UEBxMJTGEgTGFndW5hMQwwCgYDVQQKEwNVTEwxDjAMBgNVBAMTBUNo
ZXVrMScwJQYJKoZIhvcNAQkBFhhhbHUwMTAxMzY0NTQ0QHVsbC5lZHUuZXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpeQmpyQImI7ci4t2IJGhPiBhN
r14E7FbJniKHaslkPwDi3WjyxBJ//FcuPx0XSZ8Y8kNQU4PwTswSSf7TxDzs9hdn
ZVhELAbfgMJWNiFdtE8oaNn0d0l8XjxByFdwfQR5cQJHJUCs95sOXK85wQEIr/+/
B9MtTL2xmhM4wPAw8pH97uCHFTfplaCohBs2QKV8kFvzi+9bWq+zkF7gCsUu4DgB
ASVNyiPFOlT+iTlaqgVblckF6VvF3CXkpKBK5vBUhmC4lDv6hdfYqGaadyvOPiGh
ja/MyRFLmRl+YPbpnoeN6WSBI7xQGBrJuScAPERjS+d3xGY1/3UcuUg85tF5AgMB
AAGjTDBKMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBBAQDAgTwMAsGA1UdDwQEAwIF
oDAdBgNVHSUEFjAUBggrBgEFBQcDAgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQAD
ggEBAIYJ7qgUb9QcT5HWTnhIADd3lFy0KuGnq6LwWvEAtA82FTiA44KhW/chAsG5
mPS9ndcusTEG8WfzcX/gDdLt/sbneUKH3OHeu/569uXGtiK1XJvzaMY0i4jnCsHa
XTueOHfvhMvVQPTCY2zlExmssFt8pG3OBSXIZ9lJ+sVu87Ob4q3EYElczA7vpeei
pySvOd8ejt/76dioVhzFG+qapYVD9IeIlVma/N3Ti0ci3d2+8r56LI3r58aUK5wD
mbLq29oEPJX2z3a6PGziRVCSUqvNURsqV4h3z2/H/sLp6q08YJQJRZyeu2Kl8N1z
Yl6rnGxaglbsItaj2otwPPn3Zxg=
-----END CERTIFICATE-----
```

2.3. Extrae la clave pública del certificado y la clave privada del certificado cifrándola con triple des



2.4. Firma con la clave privada asociada al certificado generado el fichero DancingMan.txt



2.5. Verifica la firma que acabas de generar