

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. 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



Generar un certificado personal con getaCert

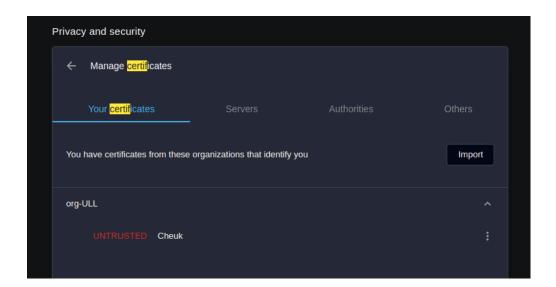


Review your self-signed certificate

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 :







2. Extrayendo información de un certificado con OpenSSL

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

```
/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:
```

```
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---
MIIDODCCArigAwIBAgIUBSMgaGfGQtxTEpFUmncwwvQX7I0wDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBhMCRVMxETAPBgNVBAgTCENhbmFyaWFzMRIwEAYDVQQHEwlM
YSBMYWd1bmExDDAKBgMVBAoTA1VMTDEOMAwGA1UEAxMFQ2h1dWsxJzA1BgkqhkiG
9w0BCQEWGGFsdTAxMDEzNjQ1NDRAdWxsLmVkdS51czAeFw0yMzEwMTMwNzQxNDBa
FwØyMzEwMTQwNzQxNDBaMHsxCzAJBgNVBAYTAkVTMREwDwYDVQQIEwhDYW5hcmlh
czESMBAGA1UEBxMJTGEgTGFndW5hMQwwCgYDVQQKEwMVTEwxDJAMBgNVBAMTBUNO
ZXVrMScwJQYJKoZIhvcNAQkBFhhhbHUwMTAxMzY9NTQ9QHVsbC51ZHUuZXMwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpeQmpyQImI7ci4t2IJGhPiBhN
T4E7FbJnikHaslkPwDi3MjyxBJ//FcuPx0XSZ8Y8kNQU4PwTsvS5F7TxDzs9hdn
ZVhELAbfgMJWNiFdtE8oaNn0d018XjxByFdwFQR5cQJHJUC395sQXK8SwQEIr/+/
B9MtTL2xmhM4wPaw8pH97uCHFTfplaCohBs2QKV8kFvzi+9bWq+zkF7gCsUu4DgB
ASWNjPF0JT+iTaqgVblckF6VvF3CXkpKBK5v8UhmC41Dv6hdfYqGaadyv0PiGh
ja/MyRFLmR1+YPbpnoeN6WSBI7xQGBrJuScAPERjS+d3xGY1/3UcuUg85tF5AgMB
AAGjTDBKMAKGA1UdEwQCMAAWEQYJYIZIAYb4QgEBBAQDAgTwMASGA1UdDwQEAWIF
oDAdBgMVHSUEFjAUBggrBgEFBQcDagYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQAD
ggEBAIYJ7qgUb9QcTSHwTnhIADd31Fy0KuGnq6LwWvEAtA82FTiA44KHW/chAsGS
 mPS9ndcusTEG8wfzcX/gDdLt/sbneUKH3OHeu/569uXGtiK1XJvzaMY0i4jnCsHa
XTueOHfvhMvVOPTCY2z1ExmssFt8pG3DBSXIZ91J+sVu870b4a3EYE1czA7vpeei
pySvOd8ejt/76dioVhzFG+qapYVD9IeI1Vma/N3TiOci3d2+8r56LI3r58aUK5wD
mbLq29oEPJX2z3a6PGziRVCSUqvNURsqV4h3z2/H/sLp6q08YJQJRZyeu2K18N1z
Y16rnGxag1bsItaj2otwPPn3Zxg=
        -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--
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQvwH4QIYp2wUJ0x348CAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECIZHPoHPr3oGBIIEyMhodxoEnrpi
kj/119poyFgKYgvrgtvdQhmI084mktn5tqKahnDG4Xz3SgrrJ512hK2py5wNed86
TdjkotLUgoCH2yuy7hWrVKekC3IoI8jH9bgocNH2x601z5ScaeWdh/0OpTeIT0Um
UDAPmmMIXKZIRPHkZFEwjb+ijoFBAT5/Obg+2fKIgyxu0IWyKR8E+Dmb3+d3cGFx
SaWFLF5kuFMGLfPCRbLGNR5Hc3xX3y2FBTup0EExIVVVBqk47b4arXZ6e1Jei1B9
xV9QjUkyeh27CIW8A7FNF/3pG1dvFuIGX3XjckRkmeKt2B1M2FNnT5haycVcp9Fs
3cYkxaVRPVf0sxShnYIJsVBDbhIoWuH1TPNudbF8q/D1CxEJkQ8TA0XhF35T5TzY
 claXboA2YgQPvHS0UWR8AI7TI0nawQuF37sSEziI8tIZnfZtK3f4P6wEkVOZdHYF
cz6va521TayVQQ8M2AimAYPkODEMDTQpZsr4kBLGbD0ODzU7aJQQhrIHxK2sFcU4
eeiHTTWvPyPhkdpiPHB2zwBqMJMpiJ5PTyi4E4gz3g84HwJC5b9C21D87uoSEohl
1F35CnGpSr7PeJTE4tfxCEZAY5/yLOiQRSJhpW0oFtifQ5ZxQ0rR9q+s08mauPQc
mcxGxSmlEs+T6avAvVEjxzOsgYfjMGJ7eBtfoCfVw98sFZp4iXSDBXn0dLm/kCls
itJFNH+01Xq+g1KZ6P5AsmeqzOfj+19jNayRJEC1XYnAogJQEKROe9LUwXhBLrXJ
ellb754ahPLa70aYo4ymEZKpL9OYH/NBDyX+ILRH5rVSAiMZlvHQZuDh6OMqvPhp
br8wfbb8U+sq8blcIm88eMJM2fIUIBoBrkSAxd0vaI+VnkapzfORpLU937rgHFHP
ngas0tQ2BHDJ/obMukWHJ8UyioOwn4kAojuLcjxZrbhuUP1Tk/hMxMwA47nrFt9y
3/XoLv+2kmgYiPbhzQ8F1ozd4QfIdvmA4/YfFTyW6NbFdwhNqvs1Dex1178BQk6m
7Dd+PLtoHw9uOcowIP6LByCfaRg71ZhXcpU9Hxp6gVz8uywBye57wHpIncD1YwAR
43GZkhp6c1KhLbvRXG8PZ1jaYKa9fuxq7xw+1yzcaguRCJmUB1MNxJsojgSsLYaB
\label{lem:ukh3CyiK7Mkwc6coq54MDEQTeCebUQw7YVIpby1PbR53scAHLeqhbb+AKZpnsmno} AOxKVDVD3V+sn6mKix011NtzBS5IkH8yqRTU8tb0YjEIVqliYQxVbq0w18JYTH+e
UBF2YOBYSLv13f4kLGuN69ReJjaDmCa9SZUJChvrTpC6M1JlmgQkd/6yy8mEVuZSL
cTczN61+syrrunCpc1Rod3RBkoF53Ky2j44PiVyaaEptdJCUVsvzkH1+pCOimVVy
Fcq6ovJjQE0L6LmSucbACRxQrkZNyB7AJt/p7RSztrMsSHyjJuM7G/DRAtUbD+3x
NVtP17UNPg/1rshz7Kpt4TLfkdBTrutggkKlh18b94ajs5xMh14obpj6gcI5+yvk
8YEou15s66/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.

```
openssl x509 -text -in certificado.pem
                  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, 0 = ULL, CN = Cheuk, emailAddress = alu0101364544@ull.edu.es

Validity

Not Reference Oct 13 07:41:40 3003 CMT
                                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:
                                                                              96:0e:3c:ar:3s:c0:101:06:ar:77:07:07:d3:2d:4c:

9d:b1:9a:13:38:c0:160:30: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:5b: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:
                                                                              d1:79
                                                               Exponent: 65537 (0x10001)
                                X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
                                                Netscape Cert Type:
SSL Client, SSL Server, S/MIME, Object Signing
               --BEGIN CERTIFICATE----
 MIIDODCCArigAwIBAgIUBsMgaGfGQtxTEpFUmncwwvQX7IGwDQYJKoZIhvcNAQEL
BQAwezELMAkGA1UEBiMCRVMxETAPBgNVBAgTCENhbmFyaWFzMRIwEAYDVQQHEwIM
YSEMYWd1bmExDDAKBgNVBAoTA1VMTDEOMAwGA1UEAxMFQ2hldWsxJzAlBgkqhkiG
9w0BCQEWGGFsdTAxMDEzNjQ1NDRAdWxsLmVkdS5lczAeFw0yMzEwMTMwNzQxNDBa
TSERHWILDHEXOLANGJAVSAN 1A.VITIUECHWAKISTICKAR (ZITCHWAKIZAK BAQRIKIS)

WOBCQEWGGFSaTTAMDEZNJQINDBAMFASCZAJBGNVBAYTAKYTMERUGWYDVQQIEWHDYWSDCSIL

FWBYMZEMTQWACZYNDBAMFASCZAJBGNVBAYTAKYTMERUGWYDVQQIEWHDYWSDCSIL

CZESMBAGALUEBXMJTGEGTGFANWSHMWHDHWWACYDVQQUEWHDYWSDCSIZHIUZXMWGGEI

MABGCSQGSID3DQEBAQUAAAIBDWAWGGEKADIBAQCPeCMppyQIMITZC:4121JGhPiBhN

r14E7FbJniKHABIAPWDi3MjyxBJ//FcuPx8VSZBYJ8KNQU4PWTSWSSf7TXDZS9HBN

ZYNELAbfqMJWNiFdtEBoaNnBddOL8XjxByFdwfQNSCQJHJUCS9SSDXX8SwGEIr/+/

B9M*TLZxmhM4wPAw8pH97uCHF1fplaCohBs2QKV8KFvzi+9bWq+zkF7gCsUu4DgB

ASVNyiPFD1T+iTlaqgVblckF6VvF3CXKpXBNSV9BUmC4LDV6HdfyQSaadyvOPiGh

JAWMSFLMR1+YPDpnoeNGWSBI7XGGBr7JSCAPENjS+d3XG71/3UcUUBgST5AMB

AAGjTDBKMAKGA1UdEwQCMAAWEQYJYIZIAYb4QGEBBAQDAgTwMAsGA1UdDwQEAwIF

ODAdBBNVHSUEFjAUBgrGBgFBQCDAgYIKwYBBQUHAWEWDQYJXOZIHVCNAQELBQAD

GJEBATYJ7QJUBOQCTSHWTNITADAGJSTJYSWKGMGDUHAWEWDQYJXOZIHVCNAQELBQAD

GJEBATYJ7QJUBOQCTSHWTNITADAGJSTJYSWKGMGDLAWVEAKBSFTIAA4KSHK/chAsGS

mPS9ndcusTEG8wfzcX/gDdLt/sbneUKH3OHeu/569uXGTiKIXJvzaMY9i4jnCSHa

XTUEOHfVhMvVQPTCYZz1Exmssft8pG3DBSXIZ9JJ+SVU870b4q3EYELczA7vpeei

DySvOR8ejt776dioVhzFG4apYVDDJEITIWan/XJTJI0ci3aGZ+FSCSLT37Vspeei

DySvOR8ejt776dioVhzFG4apYVDDJEITIWan/XJTJI0ci3aGZ+FSCSLT37SBJWSMO

mbLq290EPJX2z3a6PGziRVCSUqvNURsqV4h3z2/H/sLp6q08YJQJRZyeu2K\L8NIZ

V\GrnCxaglbsItaj2otwPPn3Zxg=

---END CERTIFICATE-----
```



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

```
/Practicas-SSI/Practica 04 Certificados y Autorid
> openssl rsa -in certificado.pem -out clave_publica.pem -pubout
Enter pass phrase for certificado.pem:
writing RSA key
                                                                                                                                                                                                                                                                                                                                               at 08:51:42
           --BEGIN PUBLIC KEY---
 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqXkJqckCJi03IuLdiCRo
T4gYTageB0xWyZ4ih2rJZD8A4t108sQSf/xXLj8dF0mfGPJDUF0D8E7MEkn+08Q8
7PYXZ2VYRCwG34DCVjYhXbRPKGjZ9HdJfF48QchXcH0EeXECRyVArPebDlyvOcEB
CK//vwfTLUy9sZoTOMDwMPKR/e7ghxU36ZWgqIQbNkClfJBb84vvWlqvs5Be4ArF
LuA4QElTcojxTpU/ok9WqoFW5XJBelbxdwl5KSgSubwVIZguJQ7+oXX2Khmmncr
zj4h0Y2vzMkRS5kZfmD26Z6HjelkgS08UBgaybknADxEY0vnd8RmNf91HLlIPObR
 eQIDAQAB
   ----END PUBLIC KEY-----
                                                                                                                                                                                                                                                                                                                                               at 08:52:48
 > openssl -in certificado.pem -des3 -out clave_privada.pem
Invalid command '-in'; type "help" for a list.
       openssl rsa -in certificado.pem -des3 -out clave_privada.pem
 Enter pass phrase for certificado.pem:
writing RSA key
 Enter pass phrase:
Verifying - Enter pass phrase:
                                                           acticas-SSI/Practica_04_Certificados_y_Autoridad_Certificadora_OpenSSL on main *1 ?1
       cat clave_privada.pem
---BEGIN ENCRYPTED PRIVATE KEY---
 MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI1U/Xwwu5jEsCAggA
MIIFHDBDBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQI1U/Xwwu5jEsCAggA
MAwGCCQGSIb3DQIJBQAwFAYIKoZIhvcNAwcECGUxKjucIChrBIIEyKI5BafvCCC8
YB88wSHTAaK8cb8IsIbymYd3BFA8B40+XkD9JfKojBaoDvluzTn63UBAyt4Xtffy
5F+8GVClh9tQVlIHV5HnPykcLfxHgi+cTqmSREsBxQsP8uDbHtdeZbUHfeRh+z9p
tBBWxD/B3ls/rX3KKRBIUWUtjy8avbPBEkmPF8RSkirIFwgs0yc5pyBL+JWvPU90
cWNV2z+gA/v4s51XWxwjFGjs8e+GbZY6b9K3AmwVR8XuzT9+RLudQXzoVw0+JKhI
RaHq71teMQCU2QG9sZXzaOele6Zku3lLUWzvClrKVD+2WPKbPQClNpSIhUjNLByf
lt6eqCaGgLBsB5nyGKE8wDpXSs0vFmAc2BtPF/ZQrliPlr2bBr+H74BYwL2POhes
2xbBb4lT49RjNyjzfNY0zo/k5E3yPfNgRNl69M0eyTrQSx7Dfni4mix0KcOccxk/
NpipPVLwoc7gIjtM6xm8syKdMoclYbp937CZkLIn4XG/wl3In9bru0UB9cVUxICC
sLGdINFYqpRe0hd9b9nU1LLIv+BaZ500pwfzHFCJVNxm53lx8GBxSds1sN8Aacut
rJu2apDs+XU3sifNre+6Yl7WIGGui3rZJusgDZaJcV7rs04pvivT0JoKP7/sH4eG
TJUZqpDs+XU3sjfNre+6Yl7WIqGui3rZJusgDZgJCV7rsQ4pyiyTQJoKP7/SH4eG
xgka/0rL3mqct80p8myg/pm+hXpuKcgBnz3ikavdg4op5+63/qm07Vbm2kUzzDTR
0WAUNgJ5tfUlrhwPQZ2s+yTs2nkIfAPSmyRFkcVwSuUc08Djc5UUcrEp3vin3v7L
Zi7XaJ60Uwj+jzlkwg6Z27WZBlHTh47Gi9MRdYGtrV8++BsL/wNViEUca1Z0foHb
Z1/XaJobowhj-j2lkwgozz/wabknii-/dusimknotkroa-stst/wkvleucalzoioho
WulvTyE6XQdHzPdW088tPN5mKXH/NSpIExtjTlccnSjVzcVv8qivFTQ5JL5Unq/I
+fpZlbFVlgyOdeEMbx+plEhtXr35fAvI/9QX02v5Qi7uU6J6l09iKK+SOHFq+V0S
NC1VhhjX+y5JiLn8lfRwzjltFrsAfQyGYkLaFeky+v2gukWrv1cYFfu0JgeP2sP4
QvZKjz8uDhOSeLjFRXoN1MnNrhN6HwWn8jaoVQtwzYkD0ZL64AbyJ1H5tJL/25F4
lUsCfJqpAS3jp8Oub5NmJAeCEMo/X7VotFUwNJwwlDzviXEyRGmS0TptzKRNdzuI
IUSCIJAGNASJ JBUUDSNMJAELEMO/X/VOTFUWNJUWLUZVIXEJROMSU JPTZKRNOZUJ JRNOPPLZB7AN/YXPYHgvJJSaetKeaeJztyJyRG++nY9cycBThSfR/K6g5/J/lry7 rm5Kgu7uAUm50rghr10bD/0QX9DE56EKJQbcpu9L60anrfwoV2j3dRojvS4PPgAW adzrTW4ms2ng1/pCeplhxfIhlyw9h7ykJ731ENBQZgGz0+ieh4nYpoS01ZJzwWTR eH9W9mcZVSEgZ5/EzASoG5oPaf/RQyAxgL5Nra/rYdVAYO+KofELSnCWJ0eioE/n uUvtrDu5GUIPUr77wuhp17WszAH9kNVhTlV8rqXDxUtdoPSa6j0Mnw4zllozN2P5 B9gnRAV9iaNQYLkAPwANMrDs/MYEONV7JWO+COaiHzYoebMVXveDxy7zj/X/KyO6
 9+bSdMhpCiSMTCLpc2Lxqv8ouqsutZcEZuGuSwBiE77gSCwGlbD+mgNZw8lYIJMy
GX1BN7KCigsFP5NvsjYkPQ==
----END ENCRYPTED PRIVATE KEY-
```



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

```
~/ / Practicas-SSI/Practica_04_Certificados y_Autoridad_Certificadora_OpenSSL_on_main *1 ?1
> openssl dgst -shal -sign clave_privada.pem -out DancingManFirmado.sig DancingMan.txt
Enter pass phrase for clave_privada.pem:

~/ / Practicas-SSI/Practica_04_Certificados_y_Autoridad_Certificadora_OpenSSL_on_main *1 ?1
> cat DancingManFirmado.sig
fq\(\hat{v}\) \(\hat{v}\) \(\hat{v}\
```

2.5. Verifica la firma que acabas de generar

~/*/Procedures /Practicas-SSI/Practica 04_Certificados y_Autoridad_Certificadora_OpenSSL_on_main *1 ?1 > openssl dgst -shal -verify clave_publica.pem -signature DancingManFirmado.sig DancingMan.txt Verified OK