Página Principal ► Mis cursos ► 192_75_601_01 : Criptografía aula 1 ► Pruebas de Evaluación Continuada (PECs) ► PEC5

Comenzado el	miércoles, 6 de mayo de 2020, 20:15
Estado	Finalizado
Finalizado en	miércoles, 6 de mayo de 2020, 21:30
Tiempo empleado	1 hora 14 minutos
Calificación	**6,08** de 10,00 (**61**%)

Pregunta 1

Parcialmente correcta

Puntúa 0,25 sobre 1,00

La página web del ayuntamiento de Barcelona (https://ajuntament.barcelona.cat/) dispone de un certificado digital que permite autenticar su identidad. Indicad el camino de certificación de este certificado digital, empezando por la entidad final y terminando en la CA raíz, es decir, indicad qué certificados habrá en este camino de certificación y en qué orden se encontrarán en el camino.

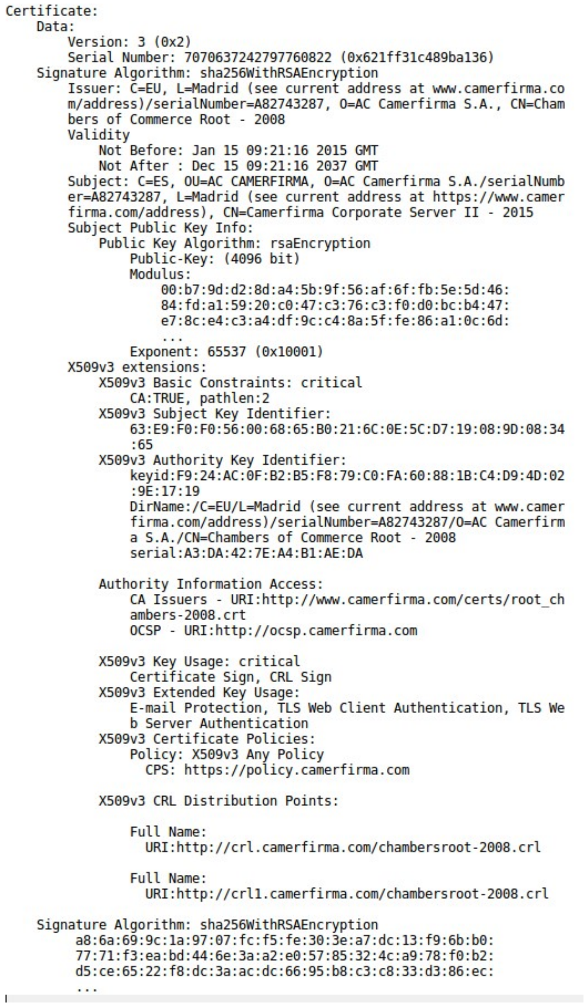
Indicad el certificado final con un 1, el certificado de la entidad que lo emite con un 2, y así sucesivamente, hasta llegar a la CA raíz. Si alguno de los certificados no se encuentra en el camino de certificación, marcad la respuesta "Este certificado no se encuentra en el camino de certificación".

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11806822484801597146 (0xa3da427ea4b1aeda)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=EU, L=Madrid (see current address at www.camerfirma.co
        m/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cham
        bers of Commerce Root - 2008
        Validity
            Not Before: Aug  1 12:29:50 2008 GMT
            Not After : Jul 31 12:29:50 2038 GMT
        Subject: C=EU, L=Madrid (see current address at www.camerfirma.c
        om/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cha
        mbers of Commerce Root - 2008
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:af:00:cb:70:37:2b:80:5a:4a:3a:6c:78:94:7d:
                    a3:7f:1a:1f:f6:35:d5:bd:db:cb:0d:44:72:3e:26:
                    b2:90:52:ba:63:3b:28:58:6f:a5:b3:6d:94:a6:f3:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:12
            X509v3 Subject Key Identifier:
                F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17
                :19
            X509v3 Authority Key Identifier:
                keyid:F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02
                :9E:17:19
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:A3:DA:42:7E:A4:B1:AE:DA

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://policy.camerfirma.com

    Signature Algorithm: sha1WithRSAEncryption
         90:12:af:22:35:c2:a3:39:f0:2e:de:e9:b5:e9:78:7c:48:be:
         3f:7d:45:92:5e:e9:da:b1:19:fc:16:3c:9f:b4:5b:66:9e:6a:
         e7:c3:b9:5d:88:e8:0f:ad:cf:23:0f:de:25:3a:5e:cc:4f:a5:
         ...
```

1 (Entidad final) ✗

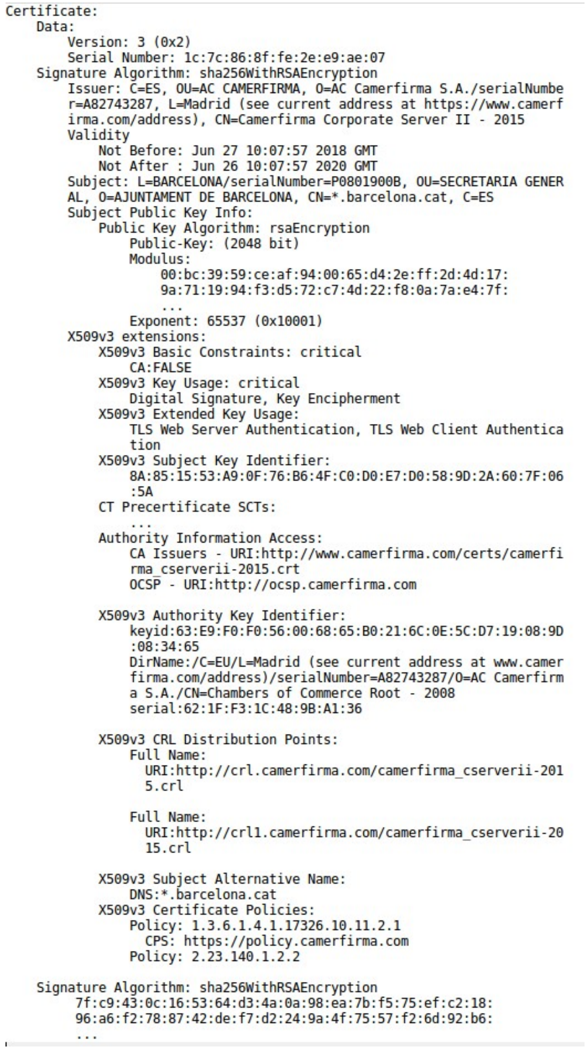
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1183638817135910154 (0x106d213ba5bfdd0a)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, OU=S
        erveis P\xC3\xBAblics de Certificaci\xC3\xB3, CN=EC-SectorPublic
        Validity
            Not Before: Apr 10 11:30:00 2018 GMT
            Not After : Apr  9 11:30:00 2020 GMT
        Subject: C=ES, ST=Barcelona, O=Consorci Administraci\xC3\xB3 Obe
        rta de Catalunya, OU=Vegeu https://www.aoc.cat/CATCert/Regulacio
        , CN=www.idcat.cat
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:c7:dc:c6:7a:10:61:bc:5e:be:3c:ae:79:5f:
                    83:58:6f:19:fd:d9:ad:31:1a:12:21:88:24:e7:66:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://www.catcert.cat/descarrega/ec-se
                ctorpublic.crt
                OCSP - URI:http://ocsp.catcert.cat

            X509v3 Subject Key Identifier:
                8E:A9:3D:81:0F:1E:BA:64:0C:C9:1E:0F:28:5B:DF:3D:1E:14:8C
                :7A
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73
                :DC:E2:D9

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.15096.1.3.1.51
                  CPS: https://www.aoc.cat/CATCert/Regulacio
                  User Notice:
                    Explicit Text: Certificat de dispositiu servidor seg
                    ur, de classe 1. Adreça i NIF del prestador: Via Lai
                    etana 26 08003 Barcelona Q0801175A

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://epscd.catcert.net/crl/ec-sectorpublic.crl

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:www.idcat.cat
            CT Precertificate SCTs:
                ...
    Signature Algorithm: sha256WithRSAEncryption
         3f:b7:fd:50:48:c5:e1:c8:af:96:83:e9:5b:a1:cf:c2:28:37:
         17:b2:87:8f:37:09:d7:f7:5d:76:ba:03:fa:a1:97:86:52:73:
         ...
```

3 ✗



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7070637242797760822 (0x621ff31c489ba136)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=EU, L=Madrid (see current address at www.camerfirma.co
        m/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cham
        bers of Commerce Root - 2008
        Validity
            Not Before: Jan 15 09:21:16 2015 GMT
            Not After : Dec 15 09:21:16 2037 GMT
        Subject: C=ES, OU=AC CAMERFIRMA, O=AC Camerfirma S.A./serialNumb
        er=A82743287, L=Madrid (see current address at https://www.camer
        firma.com/address), CN=Camerfirma Corporate Server II - 2015
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b7:9d:d2:8d:a4:5b:9f:56:af:6f:fb:5e:5d:46:
                    84:fd:a1:59:20:c0:47:c3:76:c3:f0:d0:bc:b4:47:
                    e7:8c:e4:c3:a4:df:9c:c4:8a:5f:fe:86:a1:0c:6d:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:2
            X509v3 Subject Key Identifier:
                63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34
                :65
            X509v3 Authority Key Identifier:
                keyid:F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02
                :9E:17:19
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:A3:DA:42:7E:A4:B1:AE:DA

            Authority Information Access:
                CA Issuers - URI:http://www.camerfirma.com/certs/root_ch
                ambers-2008.crt
                OCSP - URI:http://ocsp.camerfirma.com

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS We
                b Server Authentication
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://policy.camerfirma.com

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.camerfirma.com/chambersroot-2008.crl

                Full Name:
                  URI:http://crl1.camerfirma.com/chambersroot-2008.crl

    Signature Algorithm: sha256WithRSAEncryption
         a8:6a:69:9c:1a:97:07:fc:f5:fe:30:3e:a7:dc:13:f9:6b:b0:
         77:71:f3:ea:bd:44:6e:3a:a2:e0:57:85:32:4c:a9:78:f0:b2:
         d5:ce:65:22:f8:dc:3a:ac:dc:66:95:b8:c3:c8:33:d3:86:ec:
         ...
```

2 ✓



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1c:7c:86:8f:fe:2e:e9:ae:07
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, OU=AC CAMERFIRMA, O=AC Camerfirma S.A./serialNumbe
        r=A82743287, L=Madrid (see current address at https://www.camerf
        irma.com/address), CN=Camerfirma Corporate Server II - 2015
        Validity
            Not Before: Jun 27 10:07:57 2018 GMT
            Not After : Jun 26 10:07:57 2020 GMT
        Subject: L=BARCELONA/serialNumber=P0801900B, OU=SECRETARIA GENER
        AL, O=AJUNTAMENT DE BARCELONA, CN=*.barcelona.cat, C=ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bc:39:59:ce:af:94:00:65:d4:2e:ff:2d:4d:17:
                    9a:71:19:94:f3:d5:72:c7:4d:22:f8:0a:7a:e4:7f:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentica
                tion
            X509v3 Subject Key Identifier:
                8A:85:15:53:A9:0F:76:B6:4F:C0:D0:E7:D0:58:9D:2A:60:7F:06
                :5A
            CT Precertificate SCTs:
                ...
            Authority Information Access:
                CA Issuers - URI:http://www.camerfirma.com/certs/camerfi
                rma_cserverii-2015.crt
                OCSP - URI:http://ocsp.camerfirma.com

            X509v3 Authority Key Identifier:
                keyid:63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D
                :08:34:65
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:62:1F:F3:1C:48:9B:A1:36

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.camerfirma.com/camerfirma_cserverii-201
                  5.crl

                Full Name:
                  URI:http://crl1.camerfirma.com/camerfirma_cserverii-20
                  15.crl

            X509v3 Subject Alternative Name:
                DNS:*.barcelona.cat
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.17326.10.11.2.1
                  CPS: https://policy.camerfirma.com
                Policy: 2.23.140.1.2.2

    Signature Algorithm: sha256WithRSAEncryption
         7f:c9:43:0c:16:53:64:d3:4a:0a:98:ea:7b:f5:75:ef:c2:18:
         96:a6:f2:78:87:42:de:f7:d2:24:9a:4f:75:57:f2:6d:92:b6:
         ...
```

4 ✗

La teva resposta és parcialment correcta.

Ha seleccionado correctamente 1.

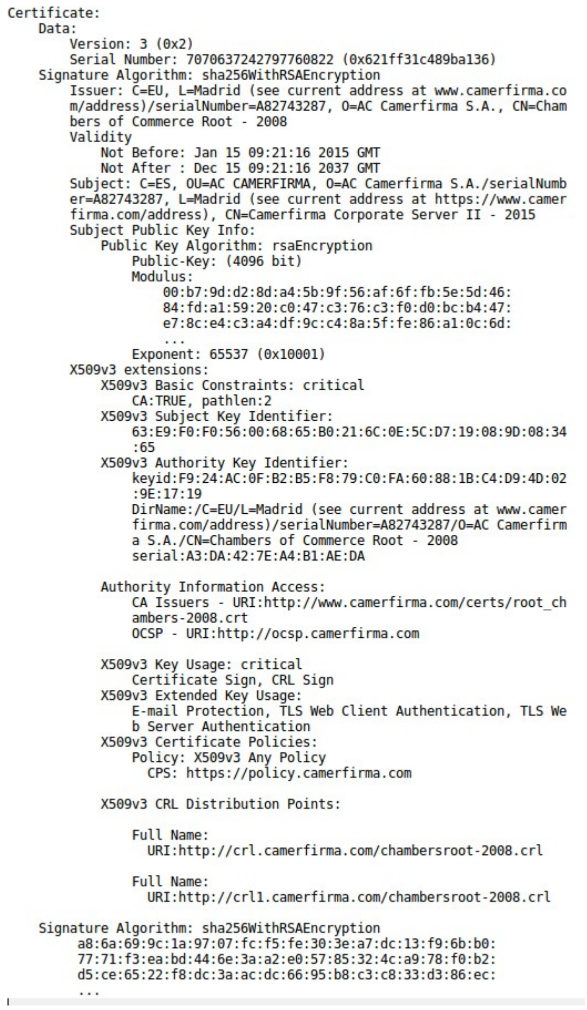
La respuesta correcta es:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 11806822484801597146 (0xa3da427ea4b1aeda)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=EU, L=Madrid (see current address at www.camerfirma.co
        m/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cham
        bers of Commerce Root - 2008
        Validity
            Not Before: Aug  1 12:29:50 2008 GMT
            Not After : Jul 31 12:29:50 2038 GMT
        Subject: C=EU, L=Madrid (see current address at www.camerfirma.c
        om/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cha
        mbers of Commerce Root - 2008
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:af:00:cb:70:37:2b:80:5a:4a:3a:6c:78:94:7d:
                    a3:7f:1a:1f:f6:35:d5:bd:db:cb:0d:44:72:3e:26:
                    b2:90:52:ba:63:3b:28:58:6f:a5:b3:6d:94:a6:f3:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:12
            X509v3 Subject Key Identifier:
                F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02:9E:17
                :19
            X509v3 Authority Key Identifier:
                keyid:F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02
                :9E:17:19
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:A3:DA:42:7E:A4:B1:AE:DA

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://policy.camerfirma.com

    Signature Algorithm: sha1WithRSAEncryption
         90:12:af:22:35:c2:a3:39:f0:2e:de:e9:b5:e9:78:7c:48:be:
         3f:7d:45:92:5e:e9:da:b1:19:fc:16:3c:9f:b4:5b:66:9e:6a:
         e7:c3:b9:5d:88:e8:0f:ad:cf:23:0f:de:25:3a:5e:cc:4f:a5:
         ...
```

→ 3,

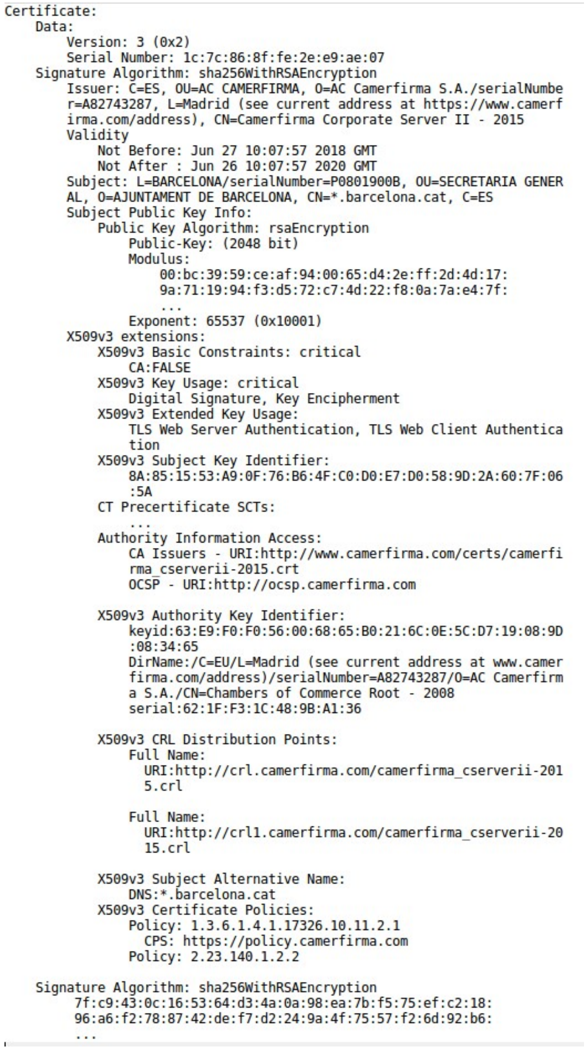
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1183638817135910154 (0x106d213ba5bfdd0a)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, O=CONSORCI ADMINISTRACIO OBERTA DE CATALUNYA, OU=S
        erveis P\xC3\xBAblics de Certificaci\xC3\xB3, CN=EC-SectorPublic
        Validity
            Not Before: Apr 10 11:30:00 2018 GMT
            Not After : Apr  9 11:30:00 2020 GMT
        Subject: C=ES, ST=Barcelona, O=Consorci Administraci\xC3\xB3 Obe
        rta de Catalunya, OU=Vegeu https://www.aoc.cat/CATCert/Regulacio
        , CN=www.idcat.cat
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:c7:dc:c6:7a:10:61:bc:5e:be:3c:ae:79:5f:
                    83:58:6f:19:fd:d9:ad:31:1a:12:21:88:24:e7:66:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://www.catcert.cat/descarrega/ec-se
                ctorpublic.crt
                OCSP - URI:http://ocsp.catcert.cat

            X509v3 Subject Key Identifier:
                8E:A9:3D:81:0F:1E:BA:64:0C:C9:1E:0F:28:5B:DF:3D:1E:14:8C
                :7A
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:
                keyid:47:3C:DE:14:77:BB:6A:4F:47:91:A9:02:FF:D4:06:E1:73
                :DC:E2:D9

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.15096.1.3.1.51
                  CPS: https://www.aoc.cat/CATCert/Regulacio
                  User Notice:
                    Explicit Text: Certificat de dispositiu servidor seg
                    ur, de classe 1. Adreça i NIF del prestador: Via Lai
                    etana 26 08003 Barcelona Q0801175A

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://epscd.catcert.net/crl/ec-sectorpublic.crl

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Alternative Name:
                DNS:www.idcat.cat
            CT Precertificate SCTs:
                ...
    Signature Algorithm: sha256WithRSAEncryption
         3f:b7:fd:50:48:c5:e1:c8:af:96:83:e9:5b:a1:cf:c2:28:37:
         17:b2:87:8f:37:09:d7:f7:5d:76:ba:03:fa:a1:97:86:52:73:
         ...
```

→ Este certificado no se encuentra en el camino de certificación.,



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 7070637242797760822 (0x621ff31c489ba136)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=EU, L=Madrid (see current address at www.camerfirma.co
        m/address)/serialNumber=A82743287, O=AC Camerfirma S.A., CN=Cham
        bers of Commerce Root - 2008
        Validity
            Not Before: Jan 15 09:21:16 2015 GMT
            Not After : Dec 15 09:21:16 2037 GMT
        Subject: C=ES, OU=AC CAMERFIRMA, O=AC Camerfirma S.A./serialNumb
        er=A82743287, L=Madrid (see current address at https://www.camer
        firma.com/address), CN=Camerfirma Corporate Server II - 2015
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b7:9d:d2:8d:a4:5b:9f:56:af:6f:fb:5e:5d:46:
                    84:fd:a1:59:20:c0:47:c3:76:c3:f0:d0:bc:b4:47:
                    e7:8c:e4:c3:a4:df:9c:c4:8a:5f:fe:86:a1:0c:6d:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:2
            X509v3 Subject Key Identifier:
                63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D:08:34
                :65
            X509v3 Authority Key Identifier:
                keyid:F9:24:AC:0F:B2:B5:F8:79:C0:FA:60:88:1B:C4:D9:4D:02
                :9E:17:19
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:A3:DA:42:7E:A4:B1:AE:DA

            Authority Information Access:
                CA Issuers - URI:http://www.camerfirma.com/certs/root_ch
                ambers-2008.crt
                OCSP - URI:http://ocsp.camerfirma.com

            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                E-mail Protection, TLS Web Client Authentication, TLS We
                b Server Authentication
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://policy.camerfirma.com

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.camerfirma.com/chambersroot-2008.crl

                Full Name:
                  URI:http://crl1.camerfirma.com/chambersroot-2008.crl

    Signature Algorithm: sha256WithRSAEncryption
         a8:6a:69:9c:1a:97:07:fc:f5:fe:30:3e:a7:dc:13:f9:6b:b0:
         77:71:f3:ea:bd:44:6e:3a:a2:e0:57:85:32:4c:a9:78:f0:b2:
         d5:ce:65:22:f8:dc:3a:ac:dc:66:95:b8:c3:c8:33:d3:86:ec:
         ...
```

→ 2,



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1c:7c:86:8f:fe:2e:e9:ae:07
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=ES, OU=AC CAMERFIRMA, O=AC Camerfirma S.A./serialNumbe
        r=A82743287, L=Madrid (see current address at https://www.camerf
        irma.com/address), CN=Camerfirma Corporate Server II - 2015
        Validity
            Not Before: Jun 27 10:07:57 2018 GMT
            Not After : Jun 26 10:07:57 2020 GMT
        Subject: L=BARCELONA/serialNumber=P0801900B, OU=SECRETARIA GENER
        AL, O=AJUNTAMENT DE BARCELONA, CN=*.barcelona.cat, C=ES
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:bc:39:59:ce:af:94:00:65:d4:2e:ff:2d:4d:17:
                    9a:71:19:94:f3:d5:72:c7:4d:22:f8:0a:7a:e4:7f:
                    ...
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentica
                tion
            X509v3 Subject Key Identifier:
                8A:85:15:53:A9:0F:76:B6:4F:C0:D0:E7:D0:58:9D:2A:60:7F:06
                :5A
            CT Precertificate SCTs:
                ...
            Authority Information Access:
                CA Issuers - URI:http://www.camerfirma.com/certs/camerfi
                rma_cserverii-2015.crt
                OCSP - URI:http://ocsp.camerfirma.com

            X509v3 Authority Key Identifier:
                keyid:63:E9:F0:F0:56:00:68:65:B0:21:6C:0E:5C:D7:19:08:9D
                :08:34:65
                DirName:/C=EU/L=Madrid (see current address at www.camer
                firma.com/address)/serialNumber=A82743287/O=AC Camerfirm
                a S.A./CN=Chambers of Commerce Root - 2008
                serial:62:1F:F3:1C:48:9B:A1:36

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.camerfirma.com/camerfirma_cserverii-201
                  5.crl

                Full Name:
                  URI:http://crl1.camerfirma.com/camerfirma_cserverii-20
                  15.crl

            X509v3 Subject Alternative Name:
                DNS:*.barcelona.cat
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.17326.10.11.2.1
                  CPS: https://policy.camerfirma.com
                Policy: 2.23.140.1.2.2

    Signature Algorithm: sha256WithRSAEncryption
         7f:c9:43:0c:16:53:64:d3:4a:0a:98:ea:7b:f5:75:ef:c2:18:
         96:a6:f2:78:87:42:de:f7:d2:24:9a:4f:75:57:f2:6d:92:b6:
         ...
```

→ 1

(Entidad final)

Pregunta 2

Correcta

Puntúa 1,00 sobre 1,00

Quién tiene que emitir el certificado para el dominio de la uoc (CN *.uoc.edu) para que nuestro navegador lo considere válido (y, por lo tanto, nos muestre la conexión en el campus como una conexión segura)?

Seleccione una:

○ a. Sólo la CA de la uoc, que es la que tiene la autoridad para hacerlo.

○ b. Sólo las CA que se encuentran explícitamente indicadas en la lista de confianza del navegador que utilizamos.

○ c. Sólo las CA subordinadas.

○ d. DigiCert, que es la única CA que emite certificados para los dominios .edu.

○ e. Cualquier CA que se encuentre dentro de la unión europea.

● f. Cualquier CA que tenga un camino de certificación hasta una CA que se encuentre en la lista de confianza del navegador que utilizamos. ✓

○ g. Cualquier CA (ya sea raíz o subordinada), que tenga un certificado con la extensión de firma de certificados.

La teva resposta és correcta.

La respuesta correcta es: Cualquier CA que tenga un camino de certificación hasta una CA que se encuentre en la lista de confianza del navegador que utilizamos.

Pregunta 3

Parcialmente correcta

Puntúa 0,50 sobre 1,00

Marcad las afirmaciones que son ciertas con relación al certificado digital siguiente:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 8793 (0x2259)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CAT, ST=Barcelona, L=Barcelona, O=UOC, OU=EIMT,
            CN=Consultor Criptografia
        Validity
            Not Before: May 23 13:27:19 2016 GMT
            Not After : May 23 13:27:19 2018 GMT
        Subject: C=CAT, ST=Barcelona, O=UOC,
            OU=EstudiantsCriptografia,
            CN=estudiant/emailAddress=estudiant@uoc.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (361 bit)
                Modulus:
                    01:b4:50:f5:bc:50:66:5e:80:0f:a3:85:07:de:c5:
                    d0:d4:36:c6:54:b1:66:db:46:49:06:37:4d:85:e2:
                    e7:b3:e8:b4:39:d7:05:77:20:67:8c:68:be:f9:37:
                    9d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                32:6C:46:E0:A5:7A:97:E3:EC:E6:0F:3D:23:14:13:7B:
                    5B:E0:97:F3
            X509v3 Authority Key Identifier:
                keyid:D2:D1:3D:A7:69:53:C6:B3:8A:10:D6:3A:51:87:
                    EB:56:4C:7C:99:7A
                DirName:/C=CAT/ST=Barcelona/L=Barcelona/
                    O=UOC/OU=EIMT/CN=Consultor Criptografia
                serial:D5:16:AD:04:20:AA:8C:26

            Netscape CA Revocation Url:
                http://www.uoc.edu/criptografia/ca-crl.pem
    Signature Algorithm: sha1WithRSAEncryption
         a4:6f:89:4e:2c:fe:85:0b:a2:7e:02:e6:45:3f:81:79:22:fa:
         2f:a1:d8:bf:43:f8:42:b9:b1:6f:6c:66:93:96:a6:2e:af:cc:
         c0:40:5f:21:69:60:77:0b:4f:00:06:40:61:f7:ad:09:1a:f2:
         1d:55:3c:a6:f5:dc:c2:f6:39:81:57:59:d6:cc:c6:b5:ad:00:
         78:be:2f:ae:d4:b6:e6:71:ab:5a:03:76:3d:0c:55:3d:87:b7:
         ab:a8:8c:2a:ef:87:09:3e:f8:50:71:b4:67:5b:a2:72:8e:a2:
         3d:3c:06:d4:09:93:c6:d7:df:4c:b3:a9:6f:ba:b2:f9:3b:95:
         44:e3:15:3c:15:ce:24:1f:23:16:c9:07:72:91:90:ff:8d:e2:
         c6:1c:95:22:18:b1:d9:39:a1:31:97:4f:cb:cc:71:23:94:4d:
         ef:0b:f0:64:3d:f7:a0:70:4c:2e:0f:6c:54:f1:95:52:00:85:
         62:9c:a3:b2:28:ea:f0:21:58:ba:4c:24:38:d7:9b:9c:78:6a:
         a6:fc:cc:11:62:11:9b:55:59:66:08:9d:98:11:3b:4c:20:e0:
         31:81:ef:1b:6d:3b:97:75:de:1f:75:6c:e5:6a:95:96:a5:9b:
         2d:f9:78:f2:31:88:f3:36:b4:21:cd:20:d4:91:e2:b0:0b:48:
         ab:fc:64:57
```

Seleccione una o más de una:

□ a. Las claves que certifica son claves RSA.

☑ b. La clave pública que se incluye se puede usar para validar firmas digitales. ✓

□ c. La firma de la CA se incluye en el certificado, y corresponde al valor 01:b4:50...

☑ d. La firma de la CA no se encuentra presente en el certificado. ✗

Las respuestas correctas son: Las claves que certifica son claves RSA., La clave pública que se incluye se puede usar para validar firmas digitales.

Pregunta 4

Correcta

Puntúa 1,00 sobre 1,00

Alice ha cifrado un mensaje usando la clave pública RSA (e,n):

e= 7

n=
7150788464000131589865412600614966001856505728792941489250523278863982808237821409567878487439894415218974698266254328695969550948326643280207526295578079

El mensaje cifrado resultante es:

2359095185102672488894038050642386820233733653433921164643078536744669.

¿Cuál es el mensaje en claro original que ha cifrado Alice?

Respuesta: 8135649109 ✓

La respuesta correcta es: 8135649109

Pregunta 5
Correcta
Puntúa 1,00 sobre 1,00

Queremos compartir el número secreto 81 entre 10 usuarios utilizando un esquema umbral (4 , 10) de compartición de secretos polinomial. Tomamos com valor para el módulo el número primo 257 y el polinomio que utilizaremos será el
$81 + 36x + 108x^2 + 185x^3$

Selecciona los fragmentos que son correctos para repartir a los usuarios.

Seleccione una o más de una:
□ a. [18,200]
□ b. [32,211]
☑ c. [17,190] ✓
☑ d. [93,203] ✓

Las respuestas correctas son: [17,190], [93,203]

Pregunta 6
Incorrecta
Puntúa 0,00 sobre 1,00

Tenemos un esquema umbral (4 , 8) de compartición de secretos polinomial y trabajamos en los enteros módulo 1913. Los fragmentos de 5 usuarios son los siguientes: [1123,751], [259,1615], [1800,1523], [355,1130], [1833,1500]

Si es posible, calcula el valor del secreto. En caso contrario escribe "NO" en la respuesta.

Respuesta:
NO

La respuesta correcta es: 597

Pregunta 7
Correcta
Puntúa 1,00 sobre 1,00

Supongamos que los usuarios A y B llevan a cabo un protocolo de tres pasos de Shamir para compartir el mensaje m=851. Para hacerlo, utilizan el criptosistema de exponenciación tal y como se describe en el apartado 1.2 del módulo 7 de la asignatura. Utilizarán como número primo el valor p=907. Suponemos que la clave para cifrar que tiene el usuario A es K_A^e = 443 y que la clave para cifrar que tiene el usuario B es K_B^e = 109. Indicad cual es el valor que el usuario A le envía al usuario B en el tercer paso del protocolo.

Respuesta: 596 ✓

La respuesta correcta es: 596

Pregunta 8
Correcta
Puntúa 1,00 sobre 1,00

Supongamos que los usuarios A y B quieren ejecutar el protocolo de firma ciega con RSA que se describe en el apartado 3.1 de módulo 7 de la asignatura. El usuario A quiere que B le firme el mensaje m=25636 sin que este conozca el contenido del mismo. Para hacerlo, utilizan el protocolo de firma ciega con RSA. La clave pública de A es (n_A=15481, e_A=5995) y su clave privada es d_A=10435. La clave pública de B es (n_B=38809, e_B=34037) y su clave privada es d_B=15405. El usuario A elige en el paso 1 del protocolo el valor r=9629. Indicad cual es el valor que el usuario B le envia al usuario A en el segundo paso del protocol.

Respuesta: 17523 ✓

La respuesta correcta es: 17523

Pregunta 9
Parcialmente correcta
Puntúa 0,33 sobre 1,00

Los usuarios A y B están ejecutando el protocolo de transferencia inconsciente 1-2. Los secretos que tiene el usuario para enviar son s_0=13883 y s_1=15325. La clave pública RSA del usuario A es (n=17473e=15417) y su clave privada d=15753. Escoge los valores correctos que se intercambiarán en cada paso del protocolo.

Paso 1 del protocolo: [x0= 8230, x1= 77] ✗

Paso 2 del protocolo: [b= 0, v= 4574] ✓

Paso 3 del protocolo: [s'0= 11563, s'1= 1606] ✗

Tu respuesta es parcialmente correcta.

Ha seleccionado correctamente 1.
La respuesta correcta es: Paso 1 del protocolo: → [x0= 979, x1= 10806] , Paso 2 del protocolo: → [b= 0, v= 4574] , Paso 3 del protocolo: → [s'0= 17962, s'1= 16166]

Pregunta 10
Incorrecta
Puntúa 0,00 sobre 1,00

El usuario A quiere demostrar a B que sabe que el logaritmo de 250 en base 3 módulo 521 vale 474, pero no quiere desvelar el valor del logaritmo. Para hacerlo, utilizará la prueba de conocimiento nulo del logaritmo discreto que está definida en el apartado 4.1 de módulo 7 de la asignatura. Suponiendo que A escoge el valor r=289 en el paso 1 del protocolo y que el usuario B escoge el bit 1 en el paso 2. Indicad cual es el valor h que el usuario A mandará a B en el paso 3 del protocolo.

Respuesta: 49 ✗

La respuesta correcta es: 243

◄ PEC4 Ir a... Máximo común divisor ►