

## Final Exam

*Duration: 2 hours*

**Documents are allowed. Calculators and other electronic devices are prohibited. The problems are independent. Show your work or otherwise justify your answers. This test is four pages long.**

### Problem I (5 points)

Andrew and Barbara want to establish a common key to be used for encrypting communications with AES. They are several thousands of miles apart with no way to meet.

1. Andrew wants to generate a 192-bit key and send it to Barbara over e-mail. Explain the security risks associated with this method and if the shortfalls can be overcome with a 256-bit key?
2. Andrew wants to use the Diffie-Hellman algorithm to establish an AES key. Barbara never heard of it before and Andrew will walk Barbara through the process, step-by-step. Provide the transcript of the e-mails between Andrew and Alice.
3. Discuss the security risk(s) associated with the procedure set out in the previous question, if any.

### Problem II (5 points)

Prove that hexadecimal number  $AA$  ( $0xAA$  for the computer scientists among you) is mapped to  $AC$  ( $0xAC$ ) with the Rijndael S-Box. Make sure to include all intermediary computations.

### Problem III (10 points)

The following description is a text dump of someone's public certificate.

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

66:ad:f5:bb:d3:e4:95:ae:1a:30:0e:b0:03:f9:0e:64

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at <https://www.verisign.com/rpa> (c)05, OU=Persona Not

Validated, CN=VeriSign Class 1 Individual Subscriber CA - G2

Validity

Not Before: Oct 8 00:00:00 2009 GMT  
 Not After : Oct 8 23:59:59 2010 GMT  
 Subject: O=VeriSign, Inc., OU=VeriSign Trust Network,  
 OU=www.verisign.com/repository/RPA Incorpor. by  
 Ref., LIAB.LTD(c)98, OU=Persona Not Validated,  
 OU=Digital ID Class 1 - Netscape Full Service,  
 CN=John Cagnol/emailAddress=john@cagnol.com  
 Subject Public Key Info:  
 Public Key Algorithm: rsaEncryption  
 RSA Public Key: (2048 bit)  
 Modulus (2048 bit):  
 00:b4:d7:6c:f0:2e:9d:cc:fe:d2:6c:e9:66:60:3b:  
 6c:06:cb:58:12:f1:13:28:c1:c5:86:a5:82:49:24:  
 8f:fd:ee:21:19:ec:35:d6:51:4a:5f:06:7c:86:2c:  
 29:9b:0e:2c:28:81:40:57:5b:60:84:b8:9a:c5:17:  
 ea:f7:47:42:92:d7:9e:43:84:be:33:c3:af:aa:57:  
 a0:b4:6c:18:fb:93:c3:bb:63:f0:1e:ff:a2:56:f4:  
 ed:c6:69:f8:bf:99:fc:6d:c6:32:93:e5:92:6f:0e:  
 9b:6d:e3:d3:d5:95:56:7a:d6:59:16:52:17:79:cb:  
 3d:0c:86:f7:a4:8a:6f:b1:df:d4:ad:4e:13:41:a5:  
 31:9c:0b:52:79:da:5c:a6:90:43:2e:6c:34:2c:25:  
 97:ce:f8:2b:1c:a7:f6:79:06:3c:d5:91:1b:35:7a:  
 4b:dc:78:b1:8a:63:6f:45:ac:b9:f7:a2:62:0b:2f:  
 39:f4:58:6f:3e:d0:08:db:c5:b4:9c:aa:91:99:65:  
 82:63:58:e6:3c:f7:83:cc:41:63:a7:37:6b:3e:f3:  
 7e:cb:42:42:e8:2b:4a:9d:2f:2b:08:d4:2f:8f:25:  
 af:09:2d:30:77:ef:cd:f4:24:c8:66:8d:a3:d4:4e:  
 47:80:5d:02:28:be:f9:6a:e0:cd:25:8d:0c:d7:42:  
 c5:2d  
 Exponent: 65537 (0x10001)  
 X509v3 extensions:  
 X509v3 Basic Constraints:  
 CA:FALSE  
 X509v3 Certificate Policies:  
 Policy: 2.16.840.1.113733.1.7.23.1  
 CPS: <https://www.verisign.com/rpa>  
 X509v3 Key Usage:  
 Digital Signature, Key Encipherment  
 X509v3 Extended Key Usage:  
 E-mail Protection, TLS Web Client Authentication  
 X509v3 CRL Distribution Points:  
 URI:<http://IndC1DigitalID-crl.verisign.com/IndC1DigitalID.crl>

Signature Algorithm: sha1WithRSAEncryption

74:bc:27:d0:a3:a0:84:8c:29:40:b7:ce:38:a7:5c:96:cc:8c:  
 bc:c2:a9:e9:44:1e:bb:4a:e4:4b:bd:3c:26:a3:53:38:d4:fe:  
 41:34:fb:42:12:2a:91:ba:77:f0:f8:70:ba:84:80:a8:cd:df:  
 ae:d2:07:4e:37:23:3f:a9:fe:99:60:24:2c:06:f8:8b:79:2b:  
 b9:4c:36:94:0e:1f:19:22:96:ba:4c:56:0c:68:f3:ed:cf:6f:  
 45:63:56:d9:41:47:88:f6:f0:fb:4f:8a:09:8b:da:46:df:9f:  
 b1:ca:a3:cc:da:a8:42:ae:e6:72:ab:03:3d:ad:19:0f:08:1c:  
 45:63:d5:ca:8c:dc:4e:5d:d8:d5:15:6b:32:54:88:46:f9:00:  
 bf:08:6c:cf:86:7c:22:0f:a9:fa:fe:c9:cc:54:7b:59:b3:6c:  
 21:85:3c:f5:c2:60:50:82:df:56:06:77:4b:2b:40:e8:ba:d2:  
 63:b5:61:3f:9e:e4:e0:6c:67:f9:a5:96:b7:59:4e:78:94:1f:  
 78:67:ba:94:88:3e:f1:bb:c0:98:3f:7c:55:6d:8f:41:fa:4c:  
 1e:52:54:b1:30:3b:f3:02:b0:1d:58:d9:da:fa:04:61:97:6d:  
 07:de:81:2f:13:5a:d6:58:76:f9:76:dc:02:53:13:41:7d:8e:  
 9e:10:d9:d6

1. What kind of certificate is it? What is the use of the certificate serial number?
2. To whom is this certificate issued and who signed it?

3. This certificate contains a validity sequence
  - a . Until when is this certificate valid?
  - b . Why is this expiration date so close?
  - c . Technically, what is the farthest date that can be set?
4.
  - a . What kind of signature algorithm is used in this certificate?
  - b . Why do we have a signature in this certificate?
  - c . Using the ASN.1 description, explain what kind of data is used to compute the certificate?
  - d . Explain in details the signature algorithm and why it cannot be forged.
5. The RDN of the issuer contains several OU fields. Is it a problem? Justify your answer.
6. This certificate contains a key.
  - a . What kind of key is it?
  - b . What is the key size?
  - c . Do you think that this key is secure enough?
  - d . Describe how this key can be used?
7. Can this certificate be used in a web browser ?

The following description is another text dump of a public certificate from that same person.

Certificate:

```

Data:
  Version: 3 (0x2)
  Serial Number:
    04:32:51:ba:78:1a:3e
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, ST=Arizona, L=Scottsdale, O=Starfield Technologies, Inc.,
    OU=http://certificates.starfieldtech.com/repository,
    CN=Starfield Secure Certification Authority/serialNumber=10688435
  Validity
    Not Before: Sep 25 04:47:27 2009 GMT
    Not After : Aug 21 17:27:04 2010 GMT
  Subject: O=cagnol.com, OU=Domain Control Validated, CN=cagnol.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
    Modulus (2048 bit):
      00:a8:e7:4d:52:bc:80:c9:8a:a1:07:ba:0a:9b:c9:
      33:e0:df:1b:77:46:f8:f5:a1:2f:b5:e2:7d:e2:f2:
      2d:a2:e4:79:bd:22:59:0f:5a:44:74:2c:12:9d:0f:
      a0:1d:bd:12:b9:09:f8:57:bc:6b:39:52:34:8b:20:
      aa:38:fb:9b:54:4a:36:8c:42:a5:08:b8:b1:3c:74:
      21:35:35:d0:77:b1:5a:46:23:e5:45:4c:8f:35:c8:
  
```

```

7b:dc:d6:f2:d3:27:41:6f:72:b6:d1:07:e7:aa:99:
ba:36:1e:4f:c7:8a:e8:1a:6e:02:26:71:61:a0:bc:
8c:d5:7e:75:e7:fb:33:ef:42:4f:66:5a:61:b9:5e:
fa:33:0f:fb:e0:aa:a3:ce:d4:70:dd:85:b1:4b:80:
cd:31:87:81:06:d4:f6:2a:1f:9c:bf:36:7e:59:3e:
66:41:f7:59:23:29:78:22:c6:98:b8:7c:47:9b:a1:
1e:b5:c3:01:a7:39:dd:da:0d:b1:0d:32:be:2a:85:
45:36:73:44:39:f4:be:59:25:80:fb:3b:e9:1e:e8:
ff:33:4e:d7:ea:df:d6:47:e8:03:e8:cd:ec:ed:f3:
ca:07:fc:76:3f:d6:7a:b3:c4:f5:e0:5f:44:17:6a:
f8:87:e9:64:f2:0d:63:d9:5a:15:e3:f7:15:a9:46:
93:b3
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Basic Constraints: critical
    CA:FALSE
  X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
  X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
  X509v3 CRL Distribution Points:
    URI:http://crl.starfieldtech.com/sfs1-0.crl

  X509v3 Certificate Policies:
    Policy: 2.16.840.1.114414.1.7.23.1
    CPS: http://certificates.starfieldtech.com/repository/

  Authority Information Access:
    OCSP - URI:http://ocsp.starfieldtech.com/
    CA Issuers - URI:http://certificates.starfieldtech.com/repository/sf_intermediate.crt

  X509v3 Authority Key Identifier:
    keyid:49:4B:52:27:D1:1B:BC:F2:A1:21:6A:62:7B:51:42:7A:8A:D7:D5:56

  X509v3 Subject Alternative Name:
    DNS:cagnol.com, DNS:www.cagnol.com
  X509v3 Subject Key Identifier:
    3C:44:DA:74:AE:2F:C8:F4:2B:97:9D:E9:15:A0:18:AD:53:F3:6D:F7
Signature Algorithm: sha1WithRSAEncryption
c8:95:b6:42:3c:bd:43:0f:b5:3a:a8:6e:30:da:c6:cd:6e:a2:
e0:f1:e1:e7:9b:13:64:88:9b:45:8c:bd:f4:b5:93:1d:d7:fb:
ba:20:89:29:d5:78:a4:5f:84:d2:1e:5c:52:cc:d7:d3:58:53:
64:00:80:d9:8a:c6:05:d4:3e:52:14:06:e6:47:65:08:e3:65:
39:aa:a9:f5:77:86:e3:7e:8e:a1:8d:de:c8:4a:62:31:6a:52:
65:05:02:3f:25:71:0f:1f:cc:da:4a:a1:97:26:19:9d:43:e5:
5b:b5:a5:96:fe:7b:1b:74:13:7f:84:fc:e3:80:a3:5f:e0:82:
c9:20:09:d1:52:d4:02:58:7b:e1:1d:a5:24:8c:b0:7a:27:4f:
66:f0:9d:1f:cf:89:c6:bc:bf:cc:84:62:e6:12:77:7c:ce:16:
bf:d0:ae:0e:fb:da:a9:27:c2:8f:09:eb:c4:6b:93:fb:fc:1a:
98:81:dd:cb:f8:cd:1d:99:db:74:aa:ae:34:45:bd:60:5e:65:
c8:1b:de:e9:81:1e:68:f3:f3:6b:f5:4b:80:80:01:83:c1:55:
9d:05:24:54:37:8d:40:46:30:e7:85:55:2f:0b:e5:2b:c0:b2:
39:4d:59:4f:ae:ff:f9:13:5f:2c:c1:c1:c2:49:69:0c:74:c5:
fe:2f:89:90

```

8. What are the differences between this one and the previous certificate?
9. Can this certificate be used in a web browser?
10. Who is concerned by these certificates?