Pôle Universitaire Léonard de Vinci
ESI GI 3906 – Cryptography

Semester 9 – Year 2008-2009
ESILV – Class of 2009

Final Exam

Duration: 2 hours

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

Problem I (8 points)

1. The following description is a text dump of a certificate installed inside the Firefox 3 browser.

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number:
           13:86:35:4d:1d:3f:06:f2:c1:f9:65:05:d5:90:1c:62
       Signature Algorithm: sha1WithRSAEncryption
       Issuer: C=US, O=VISA, OU=Visa International Service Association,
               CN=Visa eCommerce Root
       Validity
           Not Before: Jun 26 02:18:36 2002 GMT
           Not After : Jun 24 00:16:12 2022 GMT
       Subject: C=US, O=VISA, OU=Visa International Service Association,
                CN=Visa eCommerce Root
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (2048 bit)
               Modulus (2048 bit):
                   00:af:57:de:56:1e:6e:a1:da:60:b1:94:27:cb:17:
                   db:07:3f:80:85:4f:c8:9c:b6:d0:f4:6f:4f:cf:99:
                   d8:e1:db:c2:48:5c:3a:ac:39:33:c7:1f:6a:8b:26:
                   3d:2b:35:f5:48:b1:91:c1:02:4e:04:96:91:7b:b0:
                   33:f0:b1:14:4e:11:6f:b5:40:af:1b:45:a5:4a:ef:
                   7e:b6:ac:f2:a0:1f:58:3f:12:46:60:3c:8d:a1:e0:
                   7d:cf:57:3e:33:1e:fb:47:f1:aa:15:97:07:55:66:
                   a5:b5:2d:2e:d8:80:59:b2:a7:0d:b7:46:ec:21:63:
                   ff:35:ab:a5:02:cf:2a:f4:4c:fe:7b:f5:94:5d:84:
                   4d:a8:f2:60:8f:db:0e:25:3c:9f:73:71:cf:94:df:
                   4a:ea:db:df:72:38:8c:f3:96:bd:f1:17:bc:d2:ba:
                   3b:45:5a:c6:a7:f6:c6:17:8b:01:9d:fc:19:a8:2a:
                   83:16:b8:3a:48:fe:4e:3e:a0:ab:06:19:e9:53:f3:
                   80:13:07:ed:2d:bf:3f:0a:3c:55:20:39:2c:2c:00:
                   69:74:95:4a:bc:20:b2:a9:79:e5:18:89:91:a8:dc:
                   1c:4d:ef:bb:7e:37:0b:5d:fe:39:a5:88:52:8c:00:
                   6c:ec:18:7c:41:bd:f6:8b:75:77:ba:60:9d:84:e7:
                   fe:2d
               Exponent: 65537 (0x10001)
```

```
Signature Algorithm: sha1WithRSAEncryption
    5f:f1:41:7d:7c:5c:08:b9:2b:e0:d5:92:47:fa:67:5c:a5:13:
    c3:03:21:9b:2b:4c:89:46:cf:59:4d:c9:fe:a5:40:b6:63:cd:
    dd:71:28:95:67:11:cc:24:ac:d3:44:6c:71:ae:01:20:6b:03:
    a2:8f:18:b7:29:3a:7d:e5:16:60:53:78:3c:c0:af:15:83:f7:
    8f:52:33:24:bd:64:93:97:ee:8b:f7:db:18:a8:6d:71:b3:f7:
    2c:17:d0:74:25:69:f7:fe:6b:3c:94:be:4d:4b:41:8c:4e:e2:
    73:d0:e3:90:22:73:43:cd:f3:ef:ea:73:ce:45:8a:b0:a6:49:
    ff:4c:7d:9d:71:88:c4:76:1d:90:5b:1d:ee:fd:cc:f7:ee:fd:
    60:a5:b1:7a:16:71:d1:16:d0:7c:12:3c:6c:69:97:db:ae:5f:
    39:9a:70:2f:05:3c:19:46:04:99:20:36:d0:60:6e:61:06:bb:
    16:42:8c:70:f7:30:fb:e0:db:66:a3:00:01:bd:e6:2c:da:91:
    5f:a0:46:8b:4d:6a:9c:3d:3d:dd:05:46:fe:76:bf:a0:0a:3c:
    e4:00:e6:27:b7:ff:84:2d:de:ba:22:27:96:10:71:eb:22:ed:
    df:df:33:9c:cf:e3:ad:ae:8e:d4:8e:e6:4f:51:af:16:92:e0:
    5c:f6:07:0f
```

a . What kind of certificate is it?

b . In particular, to whom is this certificate issued and who signed it?

c . Until when is this certificate valid?

d . What kind of signature algorithm is used in this certificate? How is this signature computed and what kind of data is used to compute the certificate. As a reminder, the ASN.1 description of a certificate is:

```
Certificate ::= SEQUENCE {
  tbsCertificate          TBSCertificate,
  signatureAlgorithm      AlgorithmIdentifier,
  signature               BIT STRING
}
```

e . This certificate contains a key. What kind of key is it and what is its size? Do you think that this key is secure enough?

2. The ACME company is asking you to install a secure web site that will operate at the following URL: `https://store.acme.com`. After careful analysis, you recommend to have a server that operates with the TLS with a certificate signed by "Visa International Service Association".

a . Briefly describe the structure of your certificate and in particular the distinguished name for both the signer and the signee.

b . Will you be able to create the certificate with an open software like OpenSSL?

c . The ACME company is also requesting that the certificate be valid for 50 years. As a conscientious engineer, you tell them that this is a bad idea. Explain why? What will be your recommendation?

d . After paying your fee to "Visa International Service Association", a signed certificate is returned to you. Can you verify that this certificate is valid? If yes, what exactly needs to be verified? If yes, explain how you will proceed with all the data that are in your possession.

Problem II (7 points)

Alice, Bob and Mallaury want to play a simple version of poker over the Internet. This simple version of poker consists of drawing five cards, whoever has the best hands, according to poker rules, wins. Let

$$S = \{\text{Spades}, \text{Hearts}, \text{Diamonds}, \text{Clubs}\}$$

$$N = \{2, 3, 4, 5, 6, 7, 8, 9, 10, \text{Jack}, \text{Queen}, \text{King}, \text{Ace}\}$$

and D be the set of 52 cards

$$D = S \times N$$

Let f_S be defined on S by

$$f_S(\text{Spades}) = 0,\ f_S(\text{Hearts}) = 13,\ f_S(\text{Diamonds}) = 26,\ \text{and}\ f_S(\text{Clubs}) = 39$$

Let f_N be defined on N by

$$f_D(\text{Ace}) = 1,\ f_D(\text{Jack}) = 11,\ f_D(\text{Queen}) = 12,\ f_D(\text{King}) = 13,\ \text{and}\ \forall x \in [\![2, 10]\!],\ f_D(x) = x$$

Let f be defined by

$$\forall (s, n) \in D,\ f(s, n) = f_S(s) + f_N(n)$$

Step 1: Alice, Bob and Mallaury proceed as follows:

- Alice secretely chooses two very large prime numbers p_A and q_A, and a number e_A. She computes d_A such that $d_A e_A = 1 \pmod{(p_A - 1)(q_A - 1)}$.
- Bob secretely chooses two very large prime numbers p_B and q_B, and a number e_B. He computes d_B such that $d_B e_B = 1 \pmod{(p_B - 1)(q_B - 1)}$.
- Mallaury secretely chooses two very large prime numbers p_M and q_M, and a number e_M. She computes d_M such that $d_M e_M = 1 \pmod{(p_M - 1)(q_M - 1)}$.

The numbers are chosen big enough so attacks based on factorization cannot be carried out.

Step 2: Alice, Bob and Mallory meet and securely publish the product of the numbers p_i by q_i as well as e_i (where $i \in \{A, B, M\}$). Each one of them goes back home with the published numbers.

Step 3: For all x in D, Alice computes

$$f(x)^{e_B} \pmod{(p_B - 1)(q_B - 1)}$$

and sends the results to Bob in a random order.

Step 4: Bob receives a set of numbers D' from Alice. For all x in D', he computes

$$x^{e_M} \pmod{(p_M - 1)(q_M - 1)}$$

and sends the results to Mallaury in a random order.

Step 5: Mallaury receives a set of numbers D'' from Bob. For all x in D'', she computes

$$x^{e_A} \pmod{(p_A - 1)(q_A - 1)}$$

and sends the results to Alice in a random order.

Step 6: Alice receives D''' from Mallaury, she sets five numbers aside and sends the rest to Bob. She also keeps a copy of D''' for herself and sends it to Bob.

Step 7: Bob receives 47 elements of D''' from Alice (along with D'''). He takes five numbers among the 47 he received and sends the rest to Mallaury. He also keeps a copy of D''' for himself and sends the rest to Mallaury.

Step 8: Mallaury receives 42 elements of D''' from Bob (along with D''', which is what she had sent to Alice earlier). She takes five numbers among the 42 he received and sends the rest to Alice.

Step 9: Each player publishes p_i by q_i as well as d_i (where $i \in \{A, B, M\}$). They all *decrypt* the numbers they have set aside as well as the numbers they have passed to the next player. Whoever has the best hand wins.

1. Prove f is a bijection between D and $[\![1, 52]\!]$.

2. Explain how Bob can *decrypt* the numbers he has (in other words, provide the function that maps a number to a card).

3. The best possible hand in Poker is a royal flush: Ace, King, Queen, Jack and 10 of spades. Compute the probability so that five cards randomly taken out of the deck give a royal flush. Compute an approximation of the probablity that this happens 20 times in a row.

4. Alice, Bob and Mallaury play 20 times in row. Mallaury has a Royal Flush every single time. Alice and Bob begin to get suspicious that Mallaury might be cheating. Is it possible?

5. Suggest a simple modification in steps 3, 4 and 5 that makes it impossible for anyone to cheat.

Problem III (5 points)

1. For a thousand different integers a, we either have

i) $a^{2049} \equiv 1 \pmod{4099}$

ii) $a^{2049} \equiv -1 \pmod{4099}$

iii) $a^{4098} \equiv -1 \pmod{4099}$

What property can we believe 4099 has and why? How certain can we be?

2. Consider Diffie-Hellman with $p = 4099$ and $g = 4$. Assume Alice picked 2 as her random number and Bob picked 3 as his random number. What is the value of their shared secret?

3. Could we have chosen $p = 4100$ in the previous question?

Note

One can use $\binom{52}{5} = 2,598,960$ and $\log_{10}(2^{40}) \simeq 12$.