

CS 472

Network and Systems Security

Fall 2009

Final Exam

Time 2 & 1/2 hours

Open Book & Notes

Name:

Login:



**Part II:**

Assume a plain Message  $M = 4$ . Encrypt  $M$  using any (but specify which):

1. Additive Keys.

2. Multiplicative Keys

3. Exponentiative Keys.

**Question 2: 15 points**

Consider *Diffie-Hellman* with  $p=5$  and  $g=3$ . Assume Alice picked  $3$  as her random number while Bob picked  $4$  as his random number. What is the value of the shared secret between Alice and Bob following the *Diffie-Hellman* message exchange?

### Question 3: 15 points

Consider the following certificate request and the corresponding issued certificate.

Certificate Request:

Data:  
Version: 0 (0x0)  
Subject: C=US, ST=Virginia, L=Virginia Beach,  
O=ODU,  
OU=CS Department, CN=Chuck  
Cartledge/emailAddress=cs476@cs.odu.edu  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public Key: (1024 bit)  
Modulus (1024 bit):  
00:99:e3:34:a2:77:28:3d:bd:f7:71:1b:69:e8:2f:  
9a:73:f1:fc:9f:d1:f9:88:fe:d2:51:10:07:5f:56:  
fd:ab:c3:5b:fa:56:07:b5:63:d7:4a:e9:4a:84:73:  
69:4b:80:9f:39:b9:b3:a6:bb:ac:87:c2:8a:7f:4f:  
3d:34:1c:11:35:eb:d4:85:4a:aa:49:d7:9d:03:94:  
fd:f9:f5:bd:99:ea:ad:ce:1c:94:34:90:2a:a2:5b:  
ba:54:c9:1f:1a:e6:9e:8e:48:bc:99:ca:58:89:b9:  
89:ff:1a:ed:d3:6d:2e:55:61:17:ad:fa:4c:20:21:  
a2:c0:48:e8:1d:cb:d9:35:fb  
Exponent: 65537 (0x10001)  
Attributes:  
challengePassword :cairo  
unstructuredName :ODU CS Dept.  
Signature Algorithm: sha1WithRSAEncryption  
33:39:6b:ae:28:c0:b6:69:e4:78:ac:3b:89:1f:f5:32:df:42:  
3a:aa:df:e6:0a:32:e6:3a:c2:08:48:f3:b8:1f:4c:04:0c:3a:  
b4:05:35:ba:b2:15:b6:ee:b2:0e:a2:79:24:46:b9:33:38:ef:  
97:fe:df:9a:74:c2:5d:5f:f0:78:36:bf:5f:bd:12:47:4f:82:  
0c:97:7f:d0:75:9d:ef:e9:0c:2f:6a:46:b3:a3:be:68:e0:dd:  
d0:8a:51:2a:d4:f9:4f:e1:9e:71:4e:19:47:79:c7:4a:14:4a:  
be:96:5c:53:b4:01:94:4b:0a:55:38:5c:83:63:5d:96:74:c2:  
fc:01

Certificate:

Data:  
Version: 3 (0x2)  
Serial Number: 7 (0x7)  
Signature Algorithm: md5WithRSAEncryption  
Issuer: CN=Dr. Wahab, ST=Virginia,  
C=US/emailAddress=wahab@cs.odu.edu,  
O=Old Dominion University  
Validity  
Not Before: Oct 29 23:15:42 2009 GMT  
Not After : Oct 29 23:15:42 2010 GMT  
Subject: CN=cs476, ST=Virginia,  
C=US/emailAddress=cs476@cs.odu.edu,  
O=ODU, OU=CS Department  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public Key: (1024 bit)  
Modulus (1024 bit):  
00:99:e3:34:a2:77:28:3d:bd:f7:71:1b:69:e8:2f:  
9a:73:f1:fc:9f:d1:f9:88:fe:d2:51:10:07:5f:56:  
fd:ab:c3:5b:fa:56:07:b5:63:d7:4a:e9:4a:84:73:  
69:4b:80:9f:39:b9:b3:a6:bb:ac:87:c2:8a:7f:4f:  
3d:34:1c:11:35:eb:d4:85:4a:aa:49:d7:9d:03:94:  
fd:f9:f5:bd:99:ea:ad:ce:1c:94:34:90:2a:a2:5b:  
ba:54:c9:1f:1a:e6:9e:8e:48:bc:99:ca:58:89:b9:  
89:ff:1a:ed:d3:6d:2e:55:61:17:ad:fa:4c:20:21:  
a2:c0:48:e8:1d:cb:d9:35:fb  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
X509v3 Basic Constraints:  
CA:FALSE  
Signature Algorithm: md5WithRSAEncryption  
b5:47:80:e4:f1:0b:cf:f5:d1:28:02:b7:9b:a9:95:f5:b0:31:  
3e:6d:4e:5a:73:a8:b4:c0:62:2c:70:db:d3:a3:1d:fe:e7:4f:  
42:50:8f:7d:66:92:92:9a:b6:22:26:6b:0c:48:a3:ae:3c:e2:  
8c:f3





## **Question 5: 15 points**

### **Part I:**

The following is Dr. wahab's entry in the password file:

```
wahab:stg/i.0xxJ1zU:51:13:Hussein Abdel-Wahab:/home/wahab:/usr/local/bin/tcsh
```

- What is Dr. Wahab's slat?
- How UNIX lets Dr. Wahab login?
- Describe why it is helpful for Trudy to break into Dr. Wahab's account if he obtained the above entry.

**Part II:**

- Explain why source routing of the IP protocol is a security risk?

- Why it is recommended for Alice and Bob to select a new key for each session?

Question 6: 20 points

Part I:

The following is *Protocol 10* for Mutual Authentication:

```
Alice                                     Bob  
I'm Alice, f(K, AliceTimestamp) ----->  
<----- f(K, AliceTimestamp++)
```

Assume we modify this protocol as follows:

```
Alice                                     Bob  
I'm Alice, f(K, AliceTimestamp) ----->  
<----- f(K, BobTimestamp)
```

Is there any pitfall for this modification?

Part II:

Protocol 8 (below) for mutual authentication suffers from the *reflection attack*:



Explain why Protocol 11 (below) does NOT suffer from such reflection attack:

