Fun with Certificates part I

a Deep Dive into Cryptography and RSA for all ages

Brian Epstein
(he/him/his)

Institute for Advanced Study

Computer Manager, Network and Security

Information Security Officer

bepstein@ias.edu - @epepepep

The Institute for Advanced Study

Fun with Certificates part I

RSA Cryptography

May 13, 2019

Topics

- Cryptography
  - History and Concepts
  - Symmetric and Asymmetric (RSA/ECC)
- Certificates
  - Trust
  - Key Size (bit-length)
- Lab and Demonstrations

Cryptography

Goal: pass messages secretly between entities through an insecure medium

Fun with Certificates part I

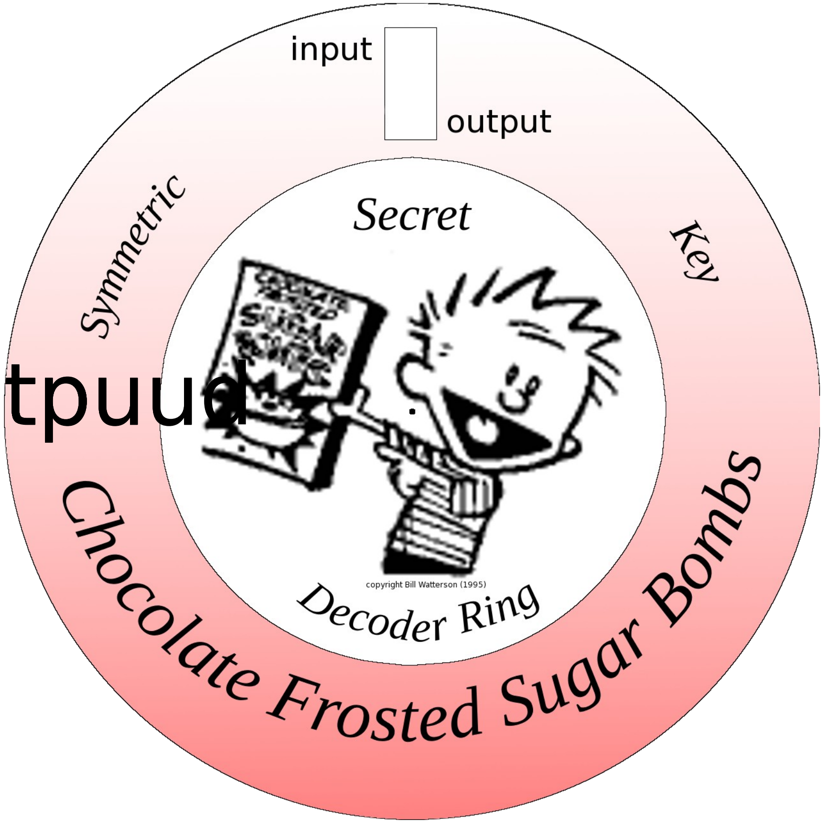
RSA Cryptography

May 13, 2019

Symmetric Cryptography

- Cereal box decoder ring/Cryptograms
- Decode secret message (“zsad”).
- Translate each letter with decoder ring
- Secret message is (“easy”).
- Reverse to encode.
- Fast.

tpuud

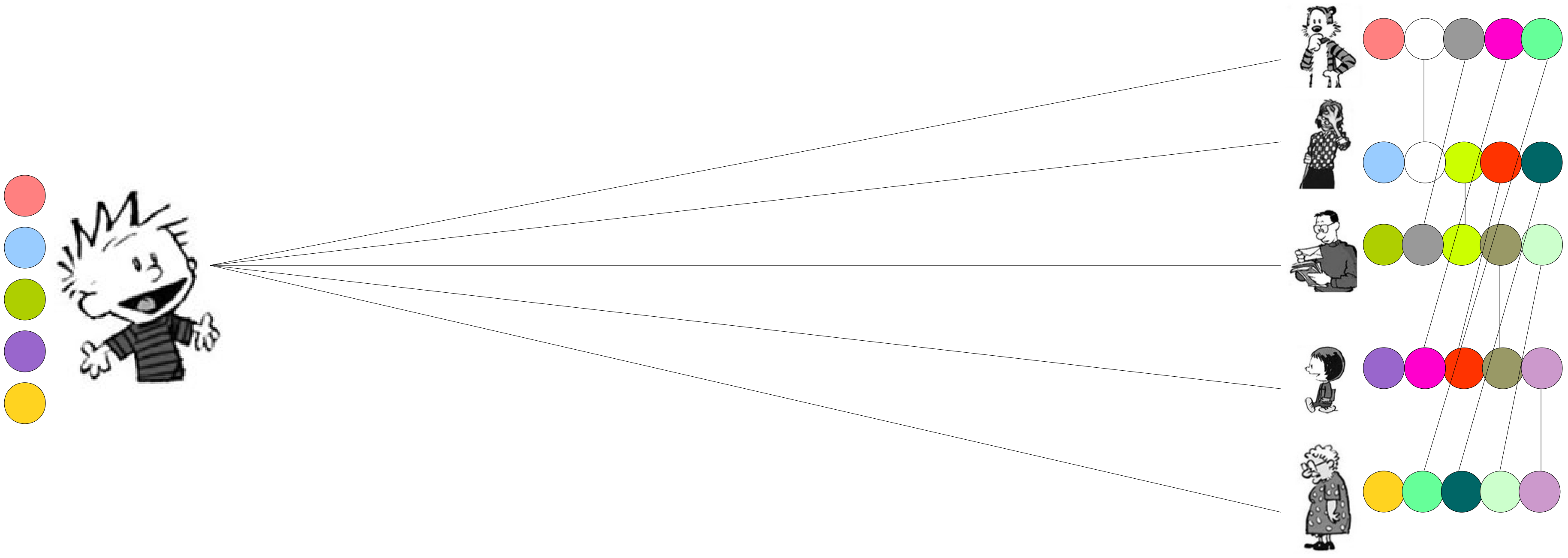

input
output
Symmetric
Secret
Key
Chocolate Frosted Sugar Bombs
Decoder Ring
copyright Bill Watterson (1995)

tpuud

Jimmy

Symmetric Box Demo

Symmetric Key Cryptography



n*(n-1)/2 = 6*(5-1)/2 = 30/2 = 15 unique keys

Fun with Certificates part I

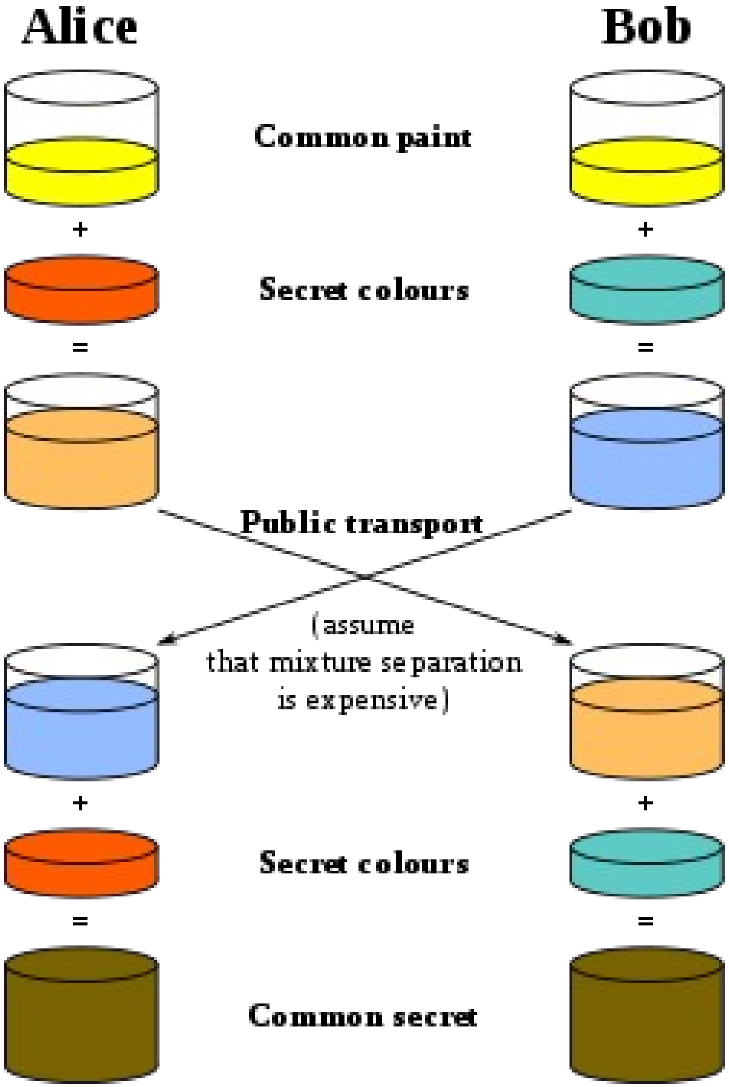
RSA Cryptography

May 13, 2019

Fun with Certificates part I

RSA Cryptography

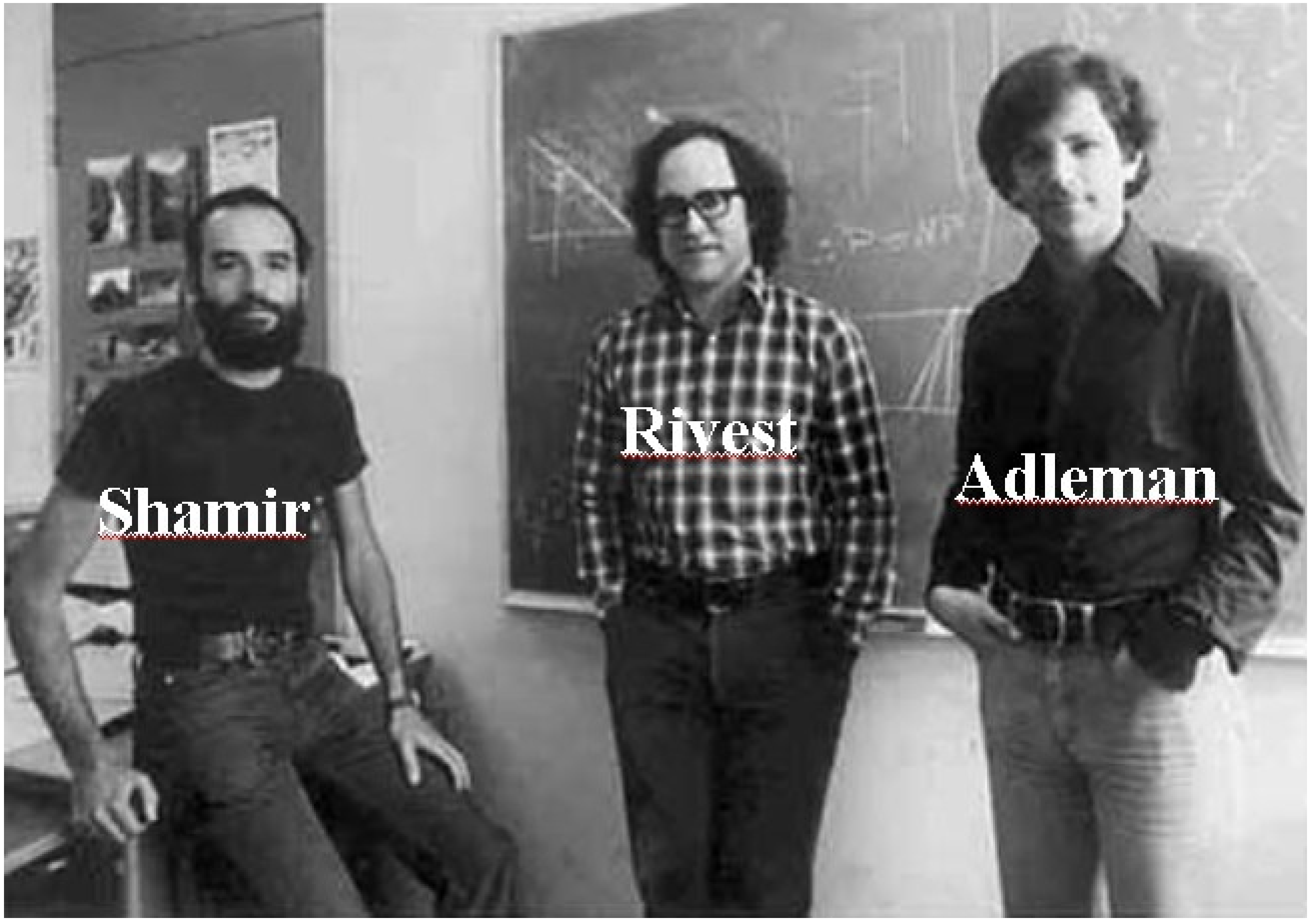
May 13, 2019



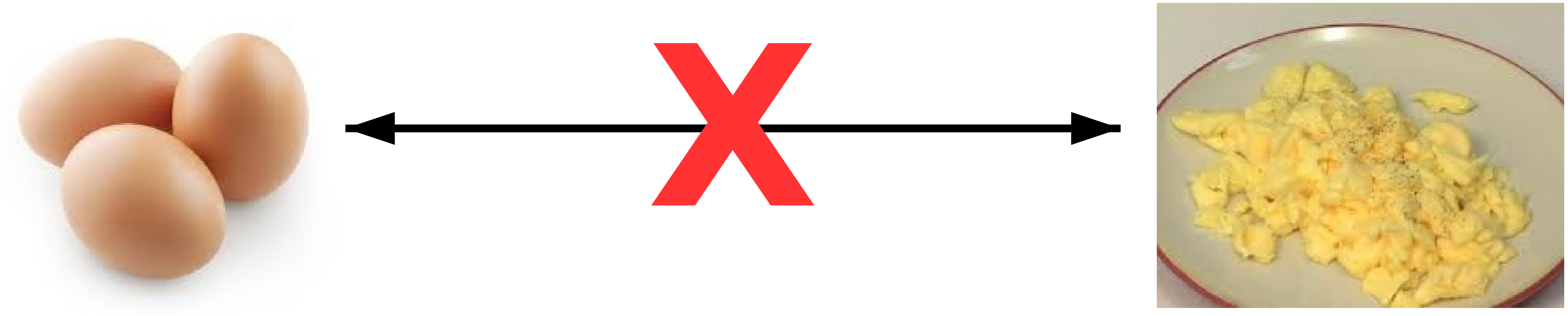
Fun with Certificates part I

RSA Cryptography

May 13, 2019



One way function



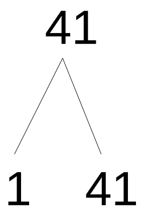
Asymmetric Keys

- Private key that you keep to yourself
- Public key that you give to everyone

Asymmetric Box Demo

Math

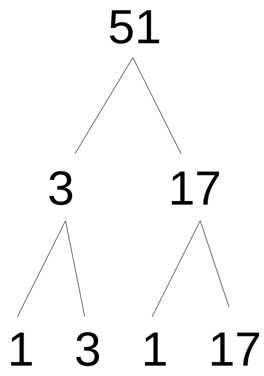
Prime Numbers



41

1 41

1 * 41 = 41



51

3 17

1 3 1 17

1 * 3 * 1 * 17 = 3 * 17 = 51

Exponents

$$\begin{aligned} 2^7 &= 2*2*2*2*2*2*2 \\ &= 128 \end{aligned}$$

2^7 = 128

Modulus

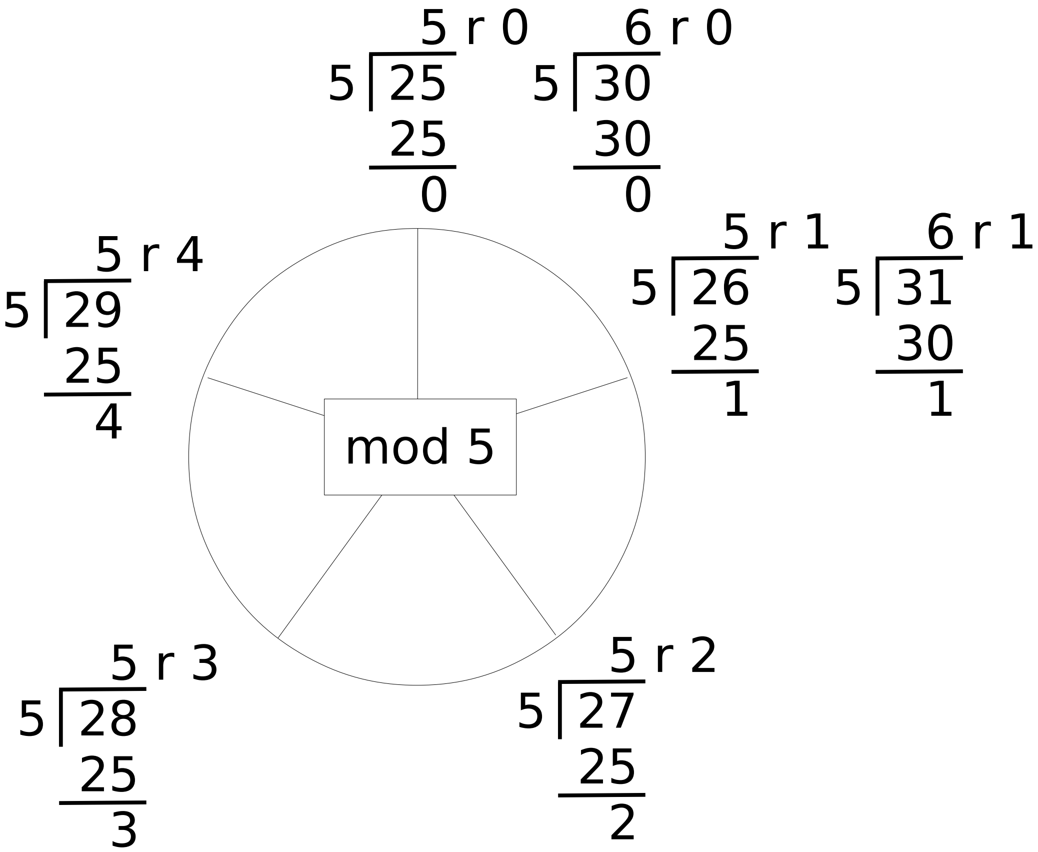
$$\begin{array}{r} 2 \text{ r } 18 \\ 55\,\overline{)\,128} \\ \underline{110} \\ 18 \end{array}$$

$$128 \div 55 = 2 \text{ r } 18$$

$$128 \bmod 55 = 18$$

$$128 \equiv 18 \pmod{55}$$

Modulus



5 r 0
5 | 25
25
0

6 r 0
5 | 30
30
0

5 r 1
5 | 26
25
1

6 r 1
5 | 31
30
1

5 r 2
5 | 27
25
2

5 r 3
5 | 28
25
3

5 r 4
5 | 29
25
4

mod 5

Fun with Certificates part I

RSA Cryptography

May 13, 2019

Modulus

- Think of modulus like a circle
- Examples
  - clock - 59 minutes becomes 0 minutes : (mod 60)
  - date - 365th day of the year becomes the 1st : (mod 365)
  - numbers - ones column goes from 9 to 0 : (mod 10)
  - circular degrees - 359° goes to 0° : (mod 360)

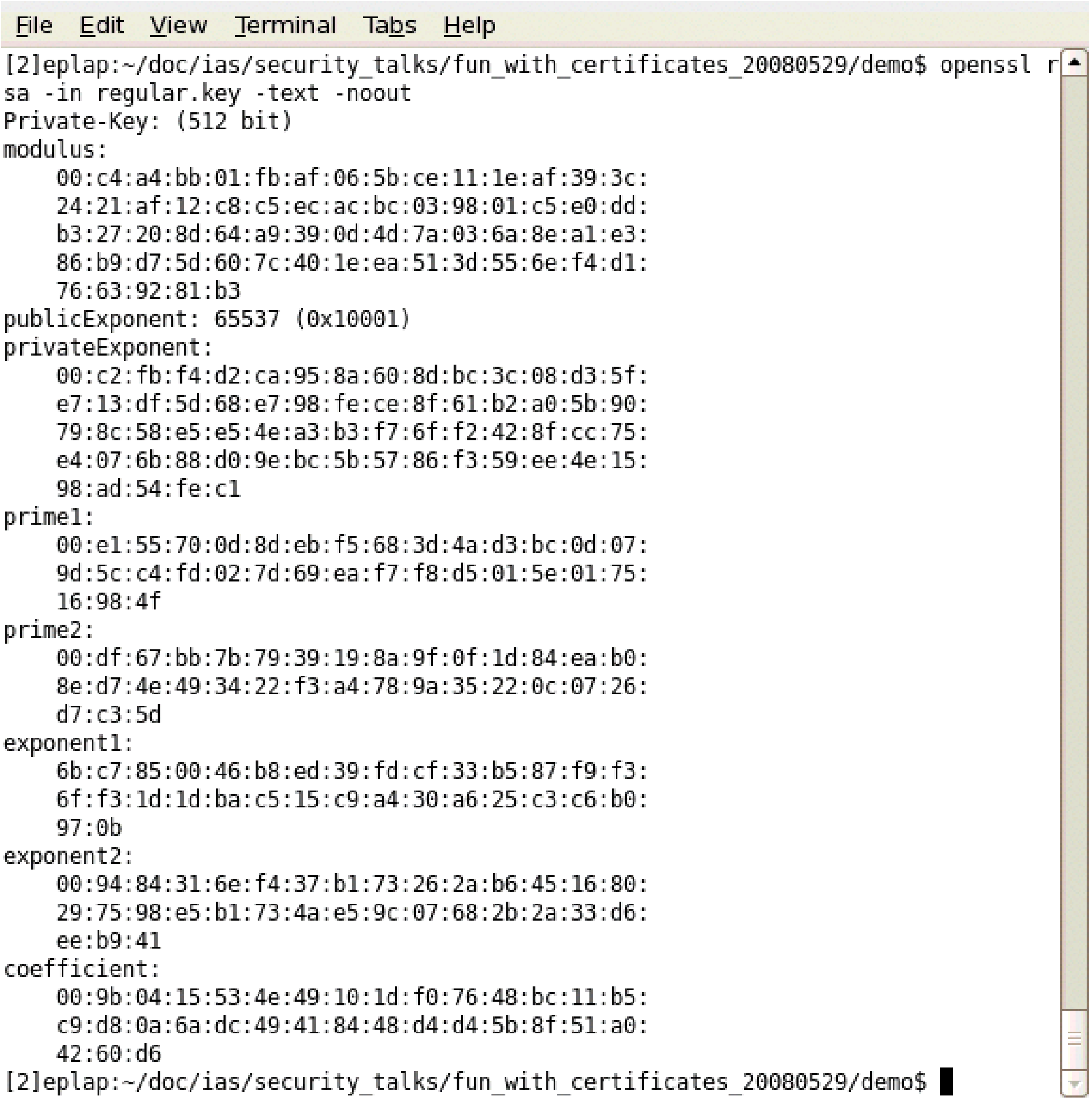
RSA Private Key Contents

- Two large Prime Numbers (p and q)
- Modulus (n = p*q)
- Private exponent (d)

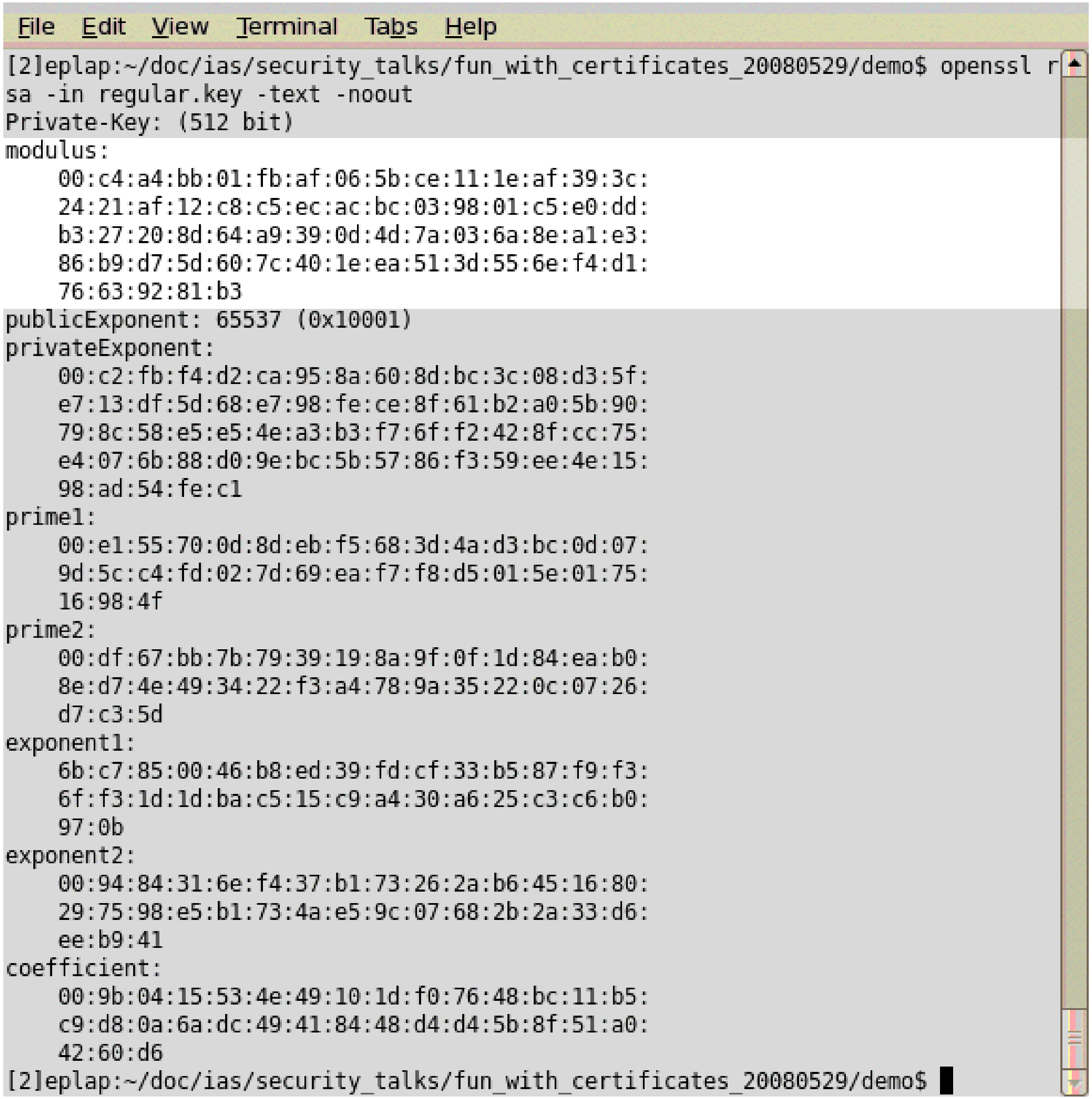
Private Exponent

- Private exponent (d) must solve

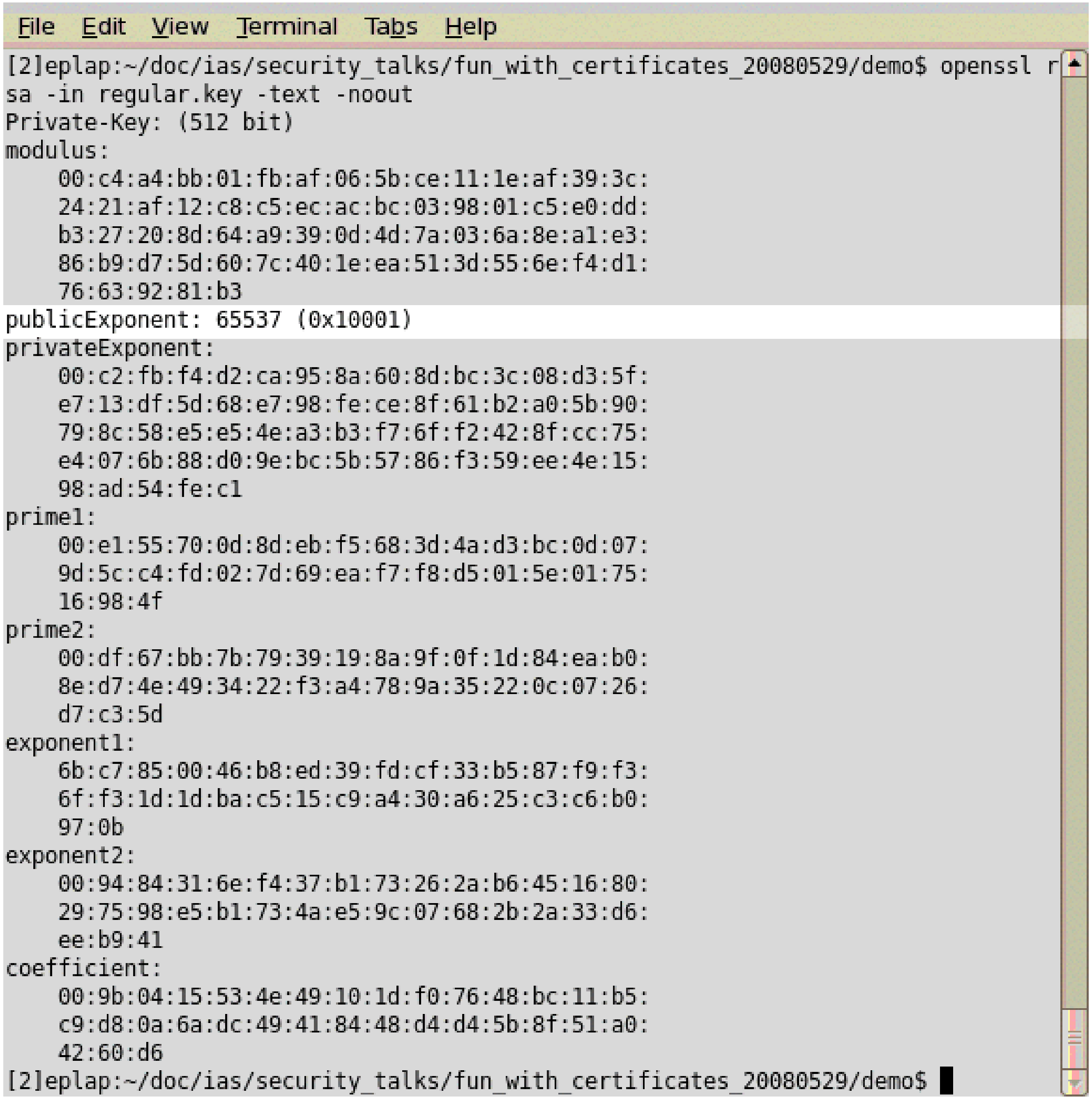
  (d*e) mod φ(n) = 1



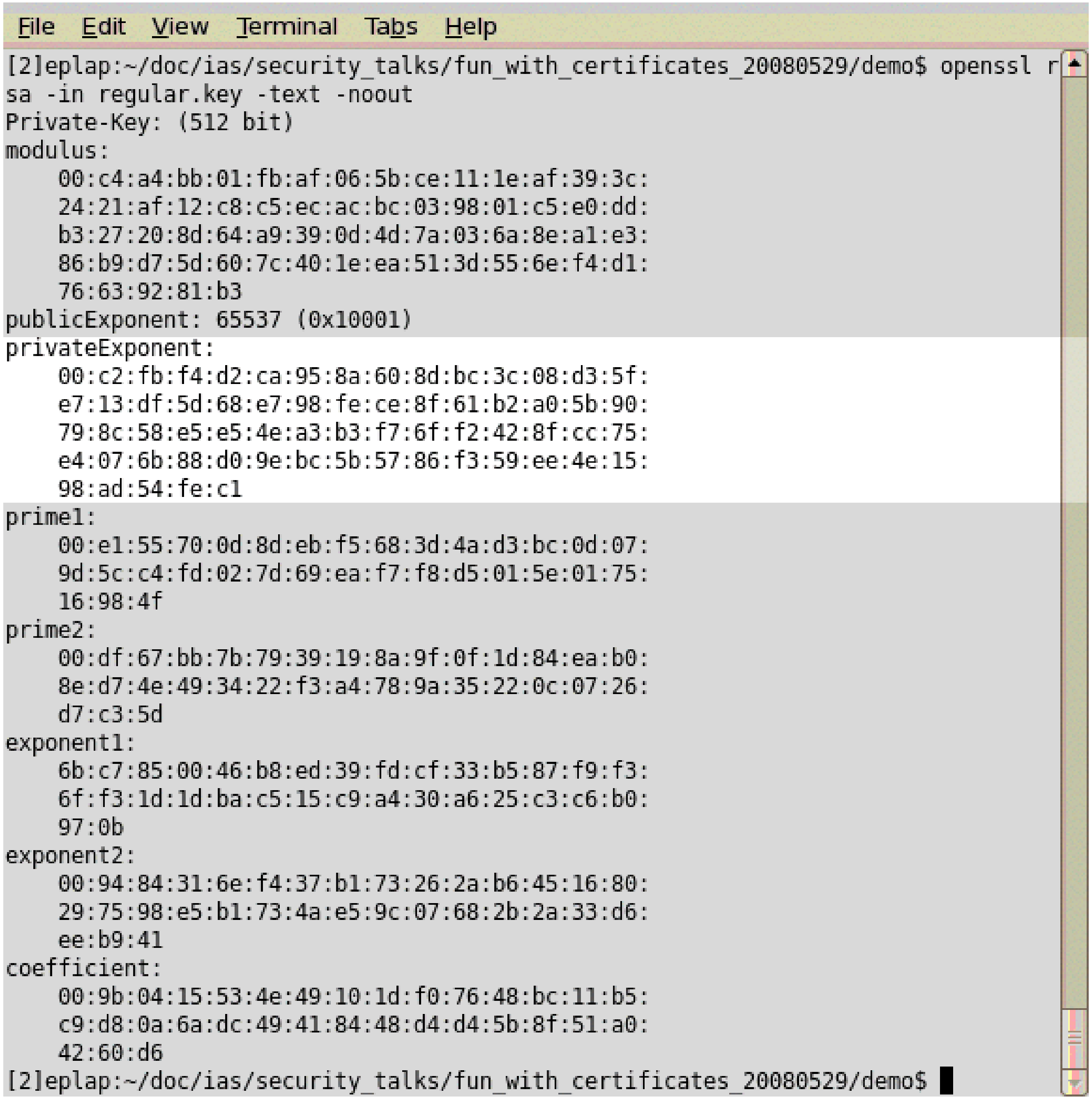
```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$
```



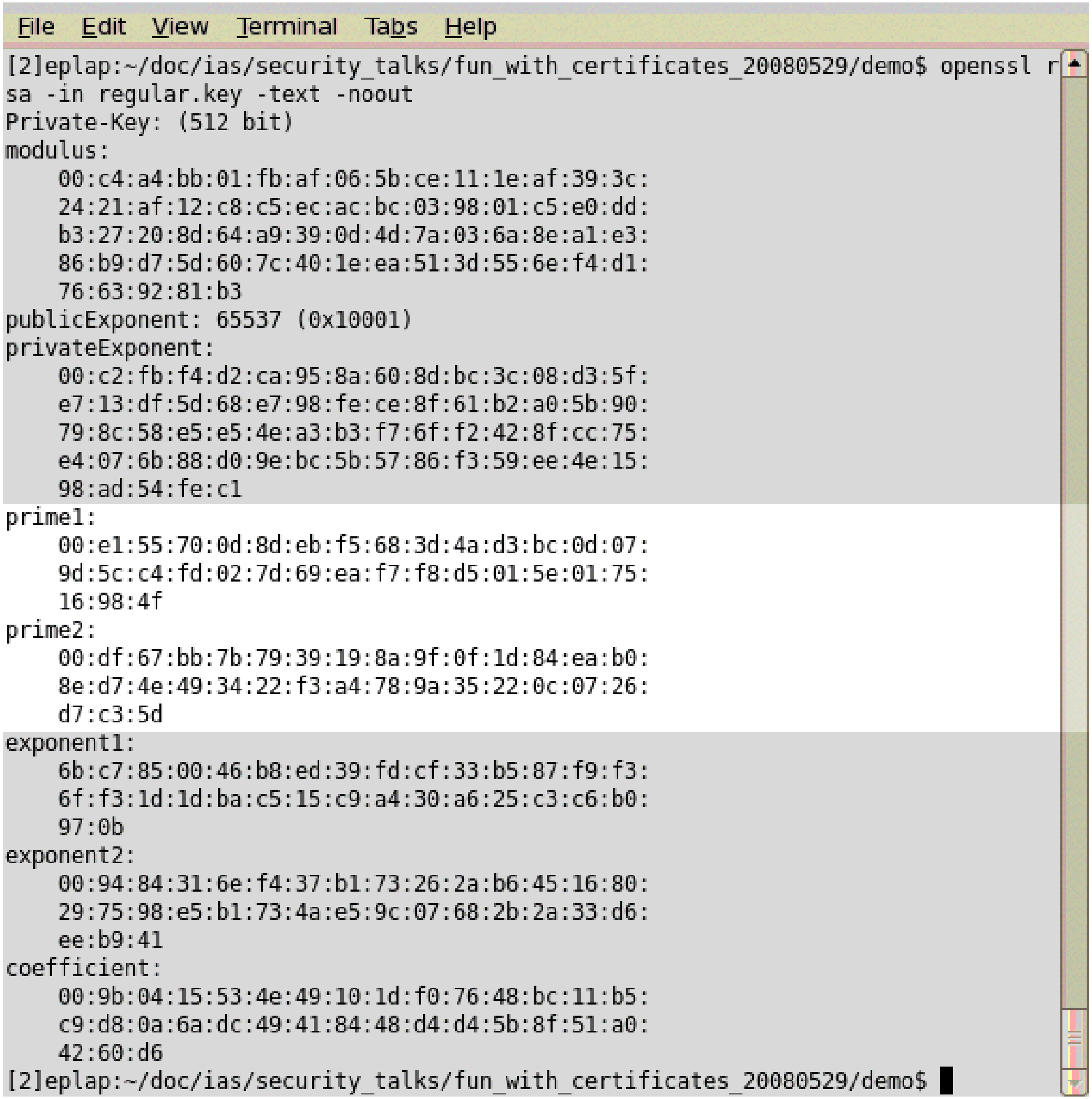
```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ 
```



```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ 
```



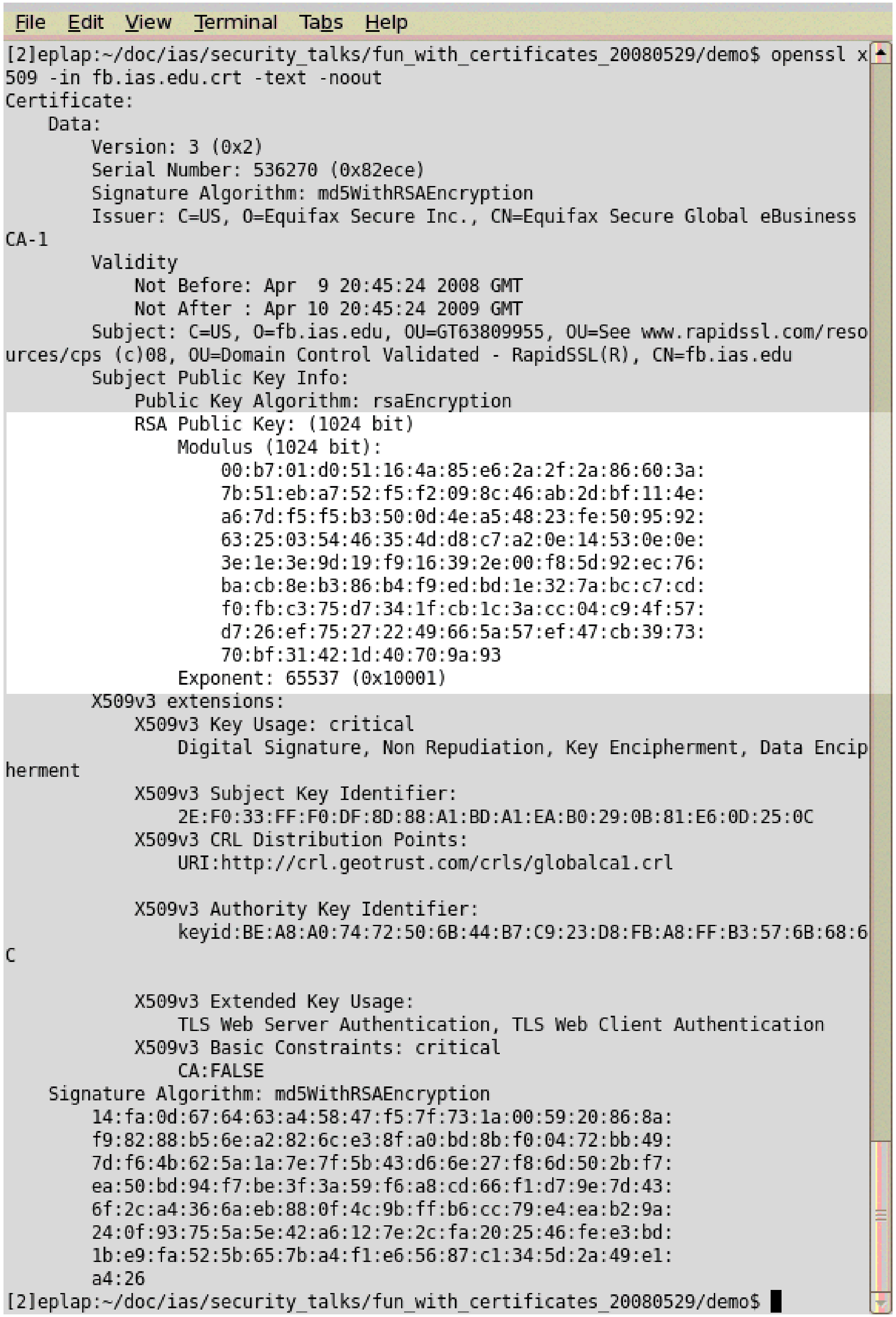
```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ 
```



```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl r
sa -in regular.key -text -noout
Private-Key: (512 bit)
modulus:
    00:c4:a4:bb:01:fb:af:06:5b:ce:11:1e:af:39:3c:
    24:21:af:12:c8:c5:ec:ac:bc:03:98:01:c5:e0:dd:
    b3:27:20:8d:64:a9:39:0d:4d:7a:03:6a:8e:a1:e3:
    86:b9:d7:5d:60:7c:40:1e:ea:51:3d:55:6e:f4:d1:
    76:63:92:81:b3
publicExponent: 65537 (0x10001)
privateExponent:
    00:c2:fb:f4:d2:ca:95:8a:60:8d:bc:3c:08:d3:5f:
    e7:13:df:5d:68:e7:98:fe:ce:8f:61:b2:a0:5b:90:
    79:8c:58:e5:e5:4e:a3:b3:f7:6f:f2:42:8f:cc:75:
    e4:07:6b:88:d0:9e:bc:5b:57:86:f3:59:ee:4e:15:
    98:ad:54:fe:c1
prime1:
    00:e1:55:70:0d:8d:eb:f5:68:3d:4a:d3:bc:0d:07:
    9d:5c:c4:fd:02:7d:69:ea:f7:f8:d5:01:5e:01:75:
    16:98:4f
prime2:
    00:df:67:bb:7b:79:39:19:8a:9f:0f:1d:84:ea:b0:
    8e:d7:4e:49:34:22:f3:a4:78:9a:35:22:0c:07:26:
    d7:c3:5d
exponent1:
    6b:c7:85:00:46:b8:ed:39:fd:cf:33:b5:87:f9:f3:
    6f:f3:1d:1d:ba:c5:15:c9:a4:30:a6:25:c3:c6:b0:
    97:0b
exponent2:
    00:94:84:31:6e:f4:37:b1:73:26:2a:b6:45:16:80:
    29:75:98:e5:b1:73:4a:e5:9c:07:68:2b:2a:33:d6:
    ee:b9:41
coefficient:
    00:9b:04:15:53:4e:49:10:1d:f0:76:48:bc:11:b5:
    c9:d8:0a:6a:dc:49:41:84:48:d4:d4:5b:8f:51:a0:
    42:60:d6
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$
```

RSA Public Key Contents

- Modulus (n)
- Public exponent (e)



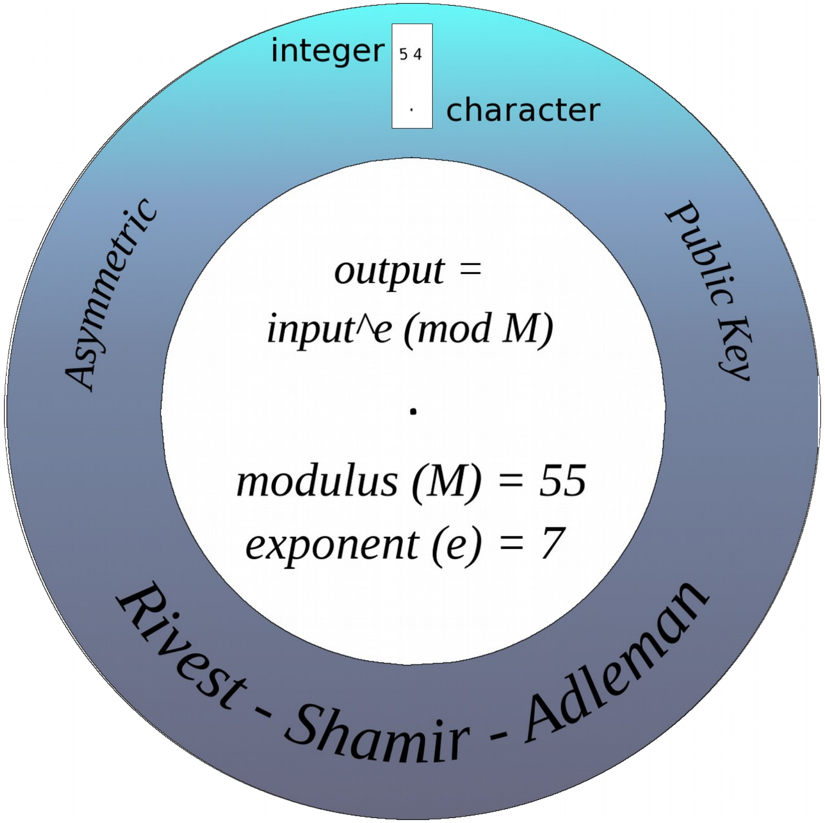
```
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ openssl x
509 -in fb.ias.edu.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 536270 (0x82ece)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, O=Equifax Secure Inc., CN=Equifax Secure Global eBusiness
CA-1
        Validity
            Not Before: Apr  9 20:45:24 2008 GMT
            Not After : Apr 10 20:45:24 2009 GMT
        Subject: C=US, O=fb.ias.edu, OU=GT63809955, OU=See www.rapidssl.com/reso
urces/cps (c)08, OU=Domain Control Validated - RapidSSL(R), CN=fb.ias.edu
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b7:01:d0:51:16:4a:85:e6:2a:2f:2a:86:60:3a:
                    7b:51:eb:a7:52:f5:f2:09:8c:46:ab:2d:bf:11:4e:
                    a6:7d:f5:f5:b3:50:0d:4e:a5:48:23:fe:50:95:92:
                    63:25:03:54:46:35:4d:d8:c7:a2:0e:14:53:0e:0e:
                    3e:1e:3e:9d:19:f9:16:39:2e:00:f8:5d:92:ec:76:
                    ba:cb:8e:b3:86:b4:f9:ed:bd:1e:32:7a:bc:c7:cd:
                    f0:fb:c3:75:d7:34:1f:cb:1c:3a:cc:04:c9:4f:57:
                    d7:26:ef:75:27:22:49:66:5a:57:ef:47:cb:39:73:
                    70:bf:31:42:1d:40:70:9a:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment, Data Encip
herment
            X509v3 Subject Key Identifier:
                2E:F0:33:FF:F0:DF:8D:88:A1:BD:A1:EA:B0:29:0B:81:E6:0D:25:0C
            X509v3 CRL Distribution Points:
                URI:http://crl.geotrust.com/crls/globalca1.crl

            X509v3 Authority Key Identifier:
                keyid:BE:A8:A0:74:72:50:6B:44:B7:C9:23:D8:FB:A8:FF:B3:57:6B:68:6
C


            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
    Signature Algorithm: md5WithRSAEncryption
        14:fa:0d:67:64:63:a4:58:47:f5:7f:73:1a:00:59:20:86:8a:
        f9:82:88:b5:6e:a2:82:6c:e3:8f:a0:bd:8b:f0:04:72:bb:49:
        7d:f6:4b:62:5a:1a:7e:7f:5b:43:d6:6e:27:f8:6d:50:2b:f7:
        ea:50:bd:94:f7:be:3f:3a:59:f6:a8:cd:66:f1:d7:9e:7d:43:
        6f:2c:a4:36:6a:eb:88:0f:4c:9b:ff:b6:cc:79:e4:ea:b2:9a:
        24:0f:93:75:5a:5e:42:a6:12:7e:2c:fa:20:25:46:fe:e3:bd:
        1b:e9:fa:52:5b:65:7b:a4:f1:e6:56:87:c1:34:5d:2a:49:e1:
        a4:26
[2]eplap:~/doc/ias/security_talks/fun_with_certificates_20080529/demo$ 
```

Public Exponent

- Public exponent (e) must be relatively prime to p-1 for all primes p which divide the modulus

One way function for RSA

Jimmy



14 13 18 18 36

One way function for RSA

14 13 18 18 36

14 13 18 18 36

One way function for RSA

14 13 18 18 36

14

13

18

18

36

One way function for RSA

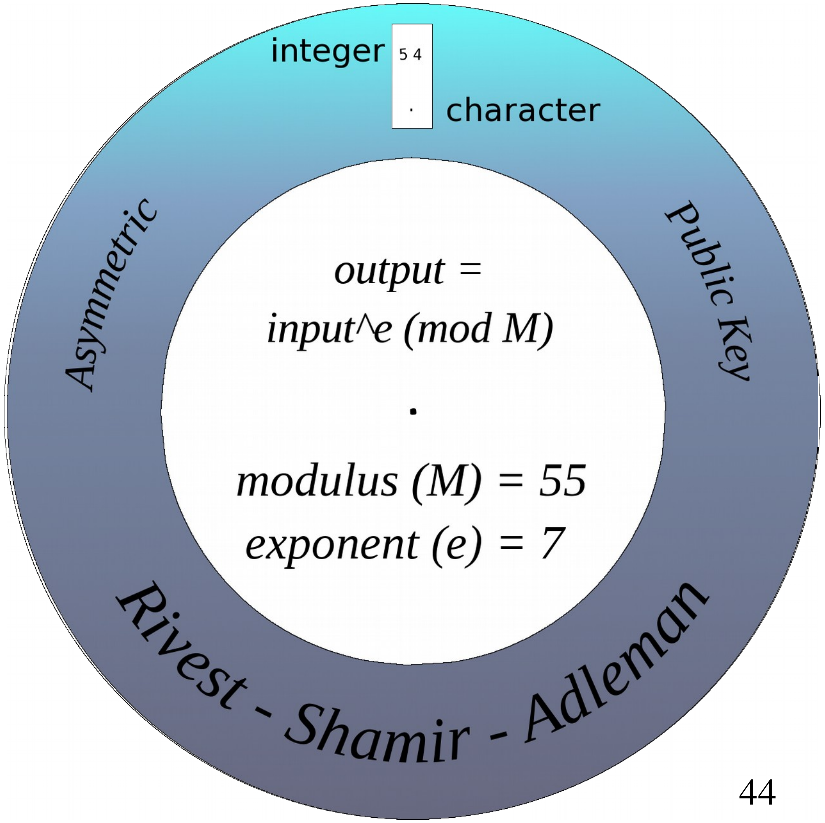
14^7 mod 55 = 105413504 mod 55 = 9 = “g”

13^7 mod 55 = 7 = “e”

18^7 mod 55 = 17 = “l”

18^7 mod 55 = 17 = “l”

36^7 mod 55 = 31 = “v”



output = input^e (mod M)

modulus (M) = 55
exponent (e) = 7

E(Jimmy) = gellv

One way function for RSA

9^{23} mod 55 = 14 = “J”

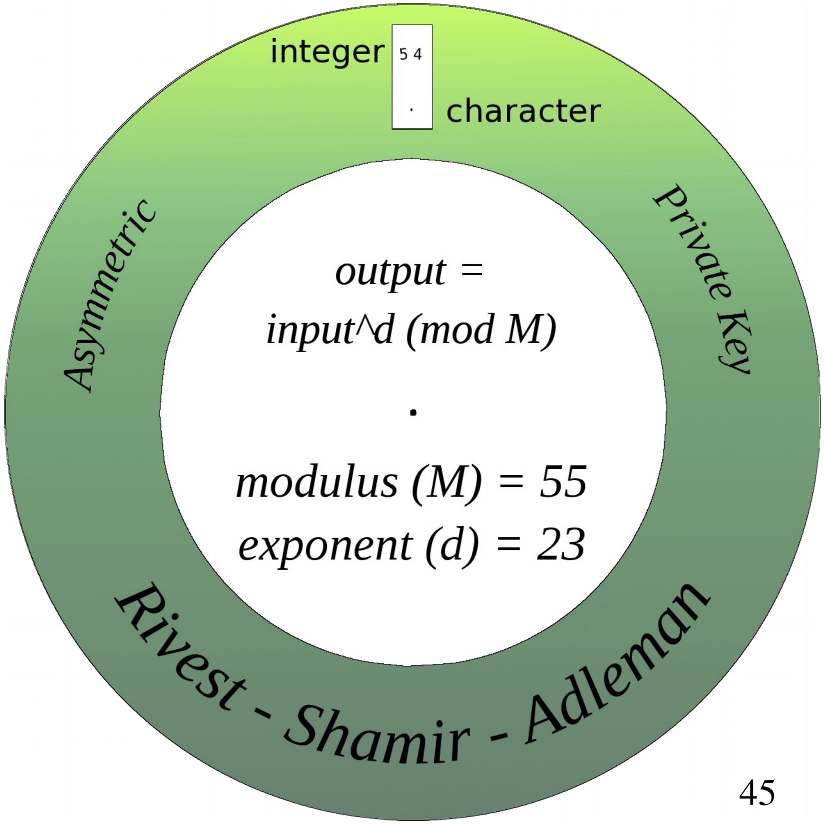
7^{23} mod 55 = 13 = “i”

17^{23} mod 55 = 18 = “m”

17^{23} mod 55 = 18 = “m”

31^{23} mod 55 = 36 = “y”

D(gellv) = Jimmy



output = *input^d (mod M)*

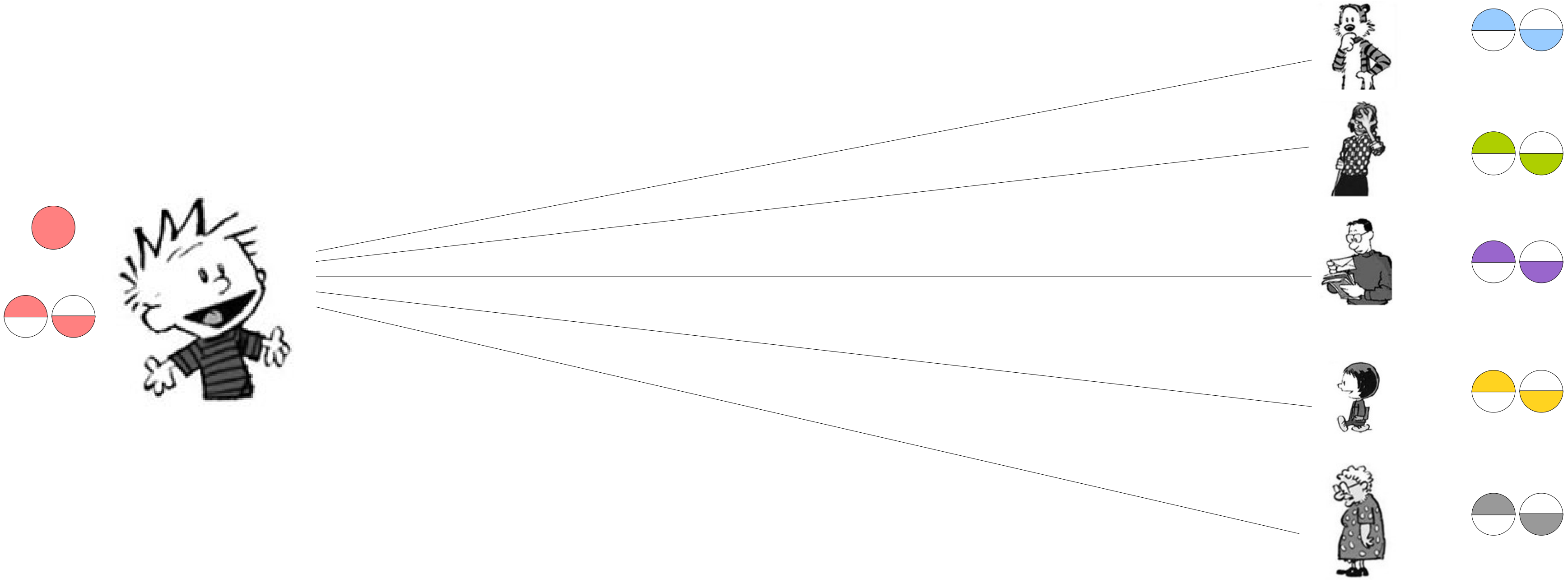
.

modulus (M) = 55
exponent (d) = 23

Asymmetric Key Demo

Modulo Calculator
https://tinyurl.com/rsacalc

Asymmetric Key Cryptography



2*n = 2 * 6 = 12 unique keys