

# LAKSHMINARAYAN KAMATH

## ABHILASHA JAIN

### PROJECT 2 REPORT

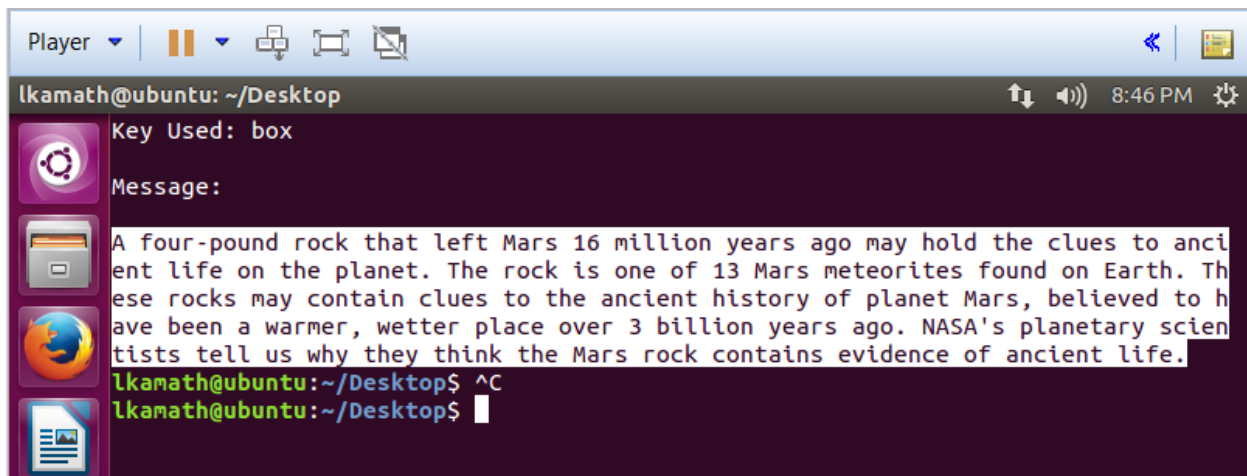
#### GOAL 1: Getting familiar with the OpenSSL Library

##### A) The secret password:

Out of  $26 \times 26 \times 26$  key combinations, only one key generated a sensible output. The key was found to be "box"

##### B) The secret message:

A four-pound rock that left Mars 16 million years ago may hold the clues to ancient life on the planet. The rock is one of 13 Mars meteorites found on Earth. These rocks may contain clues to the ancient history of planet Mars, believed to have been a warmer, wetter place over 3 billion years ago. NASA's planetary scientists tell us why they think the Mars rock contains evidence of ancient life.



```
lkamath@ubuntu: ~/Desktop
Key Used: box
Message:
A four-pound rock that left Mars 16 million years ago may hold the clues to ancient life on the planet. The rock is one of 13 Mars meteorites found on Earth. These rocks may contain clues to the ancient history of planet Mars, believed to have been a warmer, wetter place over 3 billion years ago. NASA's planetary scientists tell us why they think the Mars rock contains evidence of ancient life.
lkamath@ubuntu:~/Desktop$ ^C
lkamath@ubuntu:~/Desktop$
```

##### C) Script file :

crack.sh submitted as zip

To execute the script file, type the following command in the terminal:

```
sh crack.sh
```

## GOAL 2: Get familiar with CA and how they work

### A) A copy of our certificate in textual form

```
eos$ openssl x509 -in 101E.pem -noout -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4126 (0x101e)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, ST=NC, L=Raleigh, O=NCSU, OU=CSC, CN=574/emailAddress=harfoush@cs.ncsu.edu
    Validity
      Not Before: Nov 23 18:28:23 2015 GMT
      Not After : Nov 22 18:28:23 2016 GMT
    Subject: C=US, ST=North Carolina, L=Raleigh, O=NCSU, OU=CSC, CN=Lakshminarayan/emailAddress=lkamath@ncsu.edu
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (1024 bit)
      Modulus:
        00:e5:5e:65:62:64:a3:26:d3:45:81:a8:5e:4f:50:
        79:d0:0f:9b:b5:ae:2f:22:a1:75:d4:d1:16:08:85:
        f4:b7:e9:c2:11:b9:16:89:64:97:10:68:21:d3:66:
        38:e6:5f:cf:1c:30:de:41:4d:00:6a:2c:5a:52:8b:
        1a:95:7e:1e:83:02:28:81:2a:a0:ac:4c:11:f9:18:
        f8:33:e6:93:10:f6:ea:64:8d:0f:dd:81:52:02:5b:
        c0:6e:c4:d1:c2:5c:51:2d:f4:63:d1:6f:ad:93:c0:
        b6:1a:0e:69:03:fe:6f:82:4c:84:c4:0f:1a:f1:12:
        94:56:a8:8e:d8:60:43:c4:d5
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        OpenSSL Generated Certificate
      X509v3 Subject Key Identifier:
        B4:9B:6D:FC:27:61:4F:ED:93:21:DC:59:6B:BE:F2:02:74:10:36:41
      X509v3 Authority Key Identifier:
        keyid:AE:85:18:73:51:F3:9C:38:22:0B:55:8C:52:2F:C2:95:06:F9:9D:EF

    Signature Algorithm: sha256WithRSAEncryption
    4c:87:94:5f:25:58:c6:e6:71:87:81:93:d8:0a:59:68:fb:3d:
    a6:c1:84:13:8a:a8:68:31:70:fb:9a:e8:96:35:87:8b:54:25:
    fa:a5:f9:4c:40:00:97:72:77:8e:53:1c:02:3c:09:12:6a:3c:
    63:8f:64:bf:9e:1c:d5:c4:d0:88:90:9a:df:af:8b:16:e9:68:
    df:07:f5:6b:a0:24:c9:37:6b:6a:58:9e:0e:49:cc:74:e7:9f:
    32:54:6d:4e:0a:2f:68:8d:26:ec:de:90:95:81:eb:9c:78:ad:
    eb:83:92:3c:80:7b:04:90:68:a3:de:09:db:db:1e:e1:83:24:
    e1:e1
eos$
```

### B) Proof that we have the correct CA certificate

CA certificate fingerprint as seen in the website:

#### Root Certificate Fingerprints :

SHA1 Fingerprint EA:8A:F7:B7:4B:C7:E6:4B:59:E4:50:14:FA:88:D2:26:65:22:C4:23

MD5 Fingerprint A1:2C:26:77:A0:59:5C:55:88:10:3C:42:13:C5:62:B2

CA certificate fingerprint as obtained from openssl:

```
lkamath@engr-vcl-I-004:~/Desktop/Net Sec/Project 2/Goal 2
eos$ openssl x509 -sha1 -in root-ca.crt -noout -fingerprint
SHA1 Fingerprint=EA:8A:F7:B7:4B:C7:E6:4B:59:E4:50:14:FA:88:D2:26:65:22:C4:23
eos$ openssl x509 -md5 -in root-ca.crt -noout -fingerprint
MD5 Fingerprint=A1:2C:26:77:A0:59:5C:55:88:10:3C:42:13:C5:62:B2
eos$
```

### GOAL 3: Implementing the email security system

A) Source code submitted as Project2.zip

B) Example runs

Sender:

```
eos$ sh send_encrypt.sh
Enter your email address:
lkamath@ncsu.edu
Enter the receiver's address:
lkamath@ncsu.edu
Enter message
This is CSC 574 project 2.
Enter pass phrase for LKPrivate.pem:
eos$ █
```

Receiver:

```
eos$ sh receive_decrypt.sh
Email ID of sender:
lkamath@ncsu.edu
Enter pass phrase for LKPrivate.pem:
The message is:
This is CSC 574 project 2.
```