Team assignment for homework 1

Student IDs: 2002392,

2020 november 22

Summary

This markdown is to summarise our solutions for the first homework. Files are also available in this github repo, except for the private key in order to avoid security warnings from git.

1) Generating keys

We will generate a public-private RSA keypair for ceu.edu for which we use the PKI R package. We will save both keys in PEM format with the following code:

```
key <- PKI.genRSAkey(bits = 2048L)
prv.pem <- PKI.save.key(key, private=TRUE)
pub.pem <- PKI.save.key(key, private=FALSE)
```

2) CEU sending public key to visitors

We will write out the public and the private key as well in PEM format to disk. The same public key `id_ceu_edu.pub` will be sent to two visitors.

```
write(pub.pem, file="id_ceu_edu.pub")
write(prv.pem, file="id_ceu_edu")
```

3) Visitors create encoded message

Using the received public key, the first visitor, Visitor1 encrypts their message which is just to say hi to ceu.edu. They first load the received pub, extract it into a key object, then they use that to encrypt their message which is already converted to bytes.

```
pub.pem.loaded <- scan("id_ceu_edu.pub", what=’list’, sep=’\n’)
pub.key.loaded <- PKI.load.key(pub.pem.loaded)
message <- ’Hi ceu.edu’
bytes.to.encode = charToRaw(message)
encrypted <- PKI.encrypt(bytes.to.encode, pub.key.loaded)
```

Visitor2 does the same with their message to ceu.edu

```
pub.pem.loaded <- scan("id_ceu_edu.pub", what=’list’, sep=’\n’)
pub.key.loaded <- PKI.load.key(pub.pem.loaded)
message2 <- ’This shall be my message’
bytes.to.encode2 = charToRaw(message2)
encrypted2 <- PKI.encrypt(bytes.to.encode2, pub.key.loaded)
```

4) Visitors send message to ceu.edu

The visitors write their message to disk and send it to ceu.edu per below :

```
# First message
first_write <- file("encrypted_message.dat", "wb")
writeBin(encrypted, first_write)
close(first_write)

#Second message
second_write <- file("encrypted_message2.dat", "wb")
writeBin(encrypted2, second_write)
close(second_write)
```

5) CEU decrypting messages

ceu.edu will first read its private key from disk in PEM format and converts it to key object:

```
prv.pem.loaded <- scan("id_ceu_edu", what=’list’, sep=’\n’)
prv.key.loaded <- PKI.load.key(prv.pem.loaded)
```

ceu.edu reads both encrypted files received from visitors:

```
read.binfile <- file("encrypted_message.dat", "rb")
reread.encrypted.data <- readBin(read.binfile, raw(), n=999999999)
close(read.binfile, type = ’rb’)

read.binfile2 <- file("encrypted_message2.dat", "rb")
reread.encrypted.data2 <- readBin(read.binfile2, raw(), n=999999999)
close(read.binfile2, type = ’rb’)
```

ceu.edu then decrypts both messages and prints them to screen:

```
decrypted_message <- rawToChar(PKI.decrypt(reread.encrypted.data, prv.key.loaded))
print(decrypted_message)
```

```
## [1] "Hi ceu.edu"
```

```
decrypted_message2 <- rawToChar(PKI.decrypt(reread.encrypted.data2, prv.key.loaded))
print(decrypted_message2)
```

```
## [1] "This shall be my message"
```

Extra: print out ceu.edu’s public key in PEM format as requested in 1.d from assignment document

```
print(pub.pem.loaded)
```

```
## [1] "-----BEGIN PUBLIC KEY-----"
## [2] "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqqUCAg3vGzzfcKNgeYs2"
## [3] "e8Wd4jsw/gx7kI03BIag0v8MzsdFFZN0f/5d8VzEJ2d7sr/7Diqw9x54Xfnzdeuv"
## [4] "CyRnk3Toydl2TCcbVePqKmFH2eVHLi5ucagIPRBFGCbXjcRqjWfYe+oXSwUPqc0E"
## [5] "vJjEessZjkGfkb+nvIWhf0O1r2wfdCVmwPiKNVvE7IvTZ/febn0bSQoK/HvleNtd"
## [6] "sf/qPwuM5n0eIrUasSglUhQZDI1BJkPvISFyE3EcW/MNpEv5cvE+Zi6eGwCCERkG"
## [7] "r2HJHMGjh7D8O4XjeQd63GiOIbV6xWiUeVfWqDHKc0v3+Vi2UzZ11kSq67+JndqN"
## [8] "bwIDAQAB"
## [9] "-----END PUBLIC KEY-----"
```