DE2 - Cloud Computing Homework 1

Ersan Kucukoglu (1904225) / Haaris Afzal Cheema (2100236)

11/9/2021

a. Key generation for CEU and saving the keys in PEM format

```
keypairprovider <- PKI.genRSAkey(bits = 2048L)

prv.pem <- PKI.save.key(keypairprovider, private=TRUE)
pub.pem <- PKI.save.key(keypairprovider, private=FALSE)

ceu.pub.key <- PKI.load.key(pub.pem)
ceu.prv.key <- PKI.load.key(prv.pem)

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

By the end of this step, the public key and the private key have been generated, extracted and saved to the disk. The key will be passed to the visitor via a messenger application. The user will then try to encode a message using this public key.

b. Visitor encrypts a message with CEU's public key and writes it to disk

```
pub.pem.loaded <- scan("id_rsa_ceu.pub", what='list', sep='\n')

pub.key.loaded <- PKI.load.key(pub.pem.loaded)

encrypt <- PKI.encrypt(charToRaw("Hello CEU"), pub.key.loaded)

writeBin(encrypt, 'encoded.bin')
```

By the end of this step, the visitor has scanned the public key sent over messenger and loaded it into his r environment. The visitor then encrypts a message 'Hello CEU' and encodes it with ceu.edu's public key. This encryption is then written into a binary file and sent back to ceu.edu.

c. CEU reads back its private key from PEM along with the message, decrypts it, and prints to screen.

```
pub.pem.loaded <- scan("id_rsa_ceu.pub", what='list', sep='\n')
prv.pem.loaded <- scan("id_rsa_ceu", what='list', sep='\n')

# Extracting the key objects from the PEM file
pub.key.loaded <- PKI.load.key(pub.pem.loaded)
prv.key.loaded <- PKI.load.key(prv.pem.loaded)
```

```
encrypted_message <- readBin('encoded.bin', what=raw(), n=100000)
decrypt <- rawToChar(PKI.decrypt(encrypted_message, prv.key.loaded))
decrypt
```

```
## [1] "Hello CEU"
```

CEU uses the previously loaded private key to decrypt the encrypted message. As the output shows the actual characters and no encryption, it shows that the decryption has been done succesfully.

d. ceu.edu-s public key in PEM format (pvt key added too)

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

```
## [1] "-----BEGIN PUBLIC KEY-----"
## [2] "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAv+1IWFwDyb9iu43J8mzA"
## [3] "Vijd7W2rcSO/hW1WR4g5qYdJtBwNV0q6DhaGw4FwMqzneRjX/4rTDtHdATndx8FD"
## [4] "sUHafJ6nb9DdYNh2zIwKv2aUmZHjqTWtL2ezkCMaev4SiZgI+vh2zF4aWvaTL/Sb"
## [5] "c/zrb09EhlmbZ53760uXmGUF1zLG1tDEcVtPN+FhivJG2cRodTTXy9WlQyCtEGu4"
## [6] "BtugZFpazY5DCkJ/c2JaB02F3YmvnuUisRACq8kkJwwQb9CY0VBLdbHsS16uN9lJ"
## [7] "HfChIx3QdSO+PDfA72j/IBGmDuRFx6UDp0k1Od1nTpTC6LsY4I2TwCdk4UPwkv6P"
## [8] "/wIDAQAB"
## [9] "-----END PUBLIC KEY-----"
```

```
print(prv.pem)
```

```
##  [1] "-----BEGIN RSA PRIVATE KEY-----"
##  [2] "MIIEpAIBAAKCAQEAv+1IWFwDyb9iu43J8mzAVijd7W2rcSO/hW1WR4g5qYdJtBwN"
##  [3] "V0q6DhaGw4FwMqzneRjX/4rTDtHdATndx8FDsUHafJ6nb9DdYNh2zIwKv2aUmZHj"
##  [4] "qTWtL2ezkCMaev4SiZgI+vh2zF4aWvaTL/Sbc/zrb09EhlmbZ53760uXmGUF1zLG"
##  [5] "1tDEcVtPN+FhivJG2cRodTTXy9WlQyCtEGu4BtugZFpazY5DCkJ/c2JaB02F3Ymv"
##  [6] "nuUisRACq8kkJwwQb9CY0VBLdbHsS16uN9lJHfChIx3QdSO+PDfA72j/IBGmDuRF"
##  [7] "x6UDp0k1Od1nTpTC6LsY4I2TwCdk4UPwkv6P/wIDAQABAoIBAD5vqsFT7ceMA0qQ"
##  [8] "bcn3pvpggRHkQ4mi34NAdnj+0ANeh5OYLJ7hKHW8zkp7qUxTA1pZwqrXNqHzk7n6"
##  [9] "YTPCo4reqX0w/7dYcyw2Py97v2NUs7LhyvYZCCYLzlZtlQe977njQ8ihW8RQOLKu"
## [10] "1GMdaBTriovDdb9fFzc2JeX9yWtBoUSl7BlO8Z4Y5eoSCkYT1klLrhT/jy/6Wwg+"
## [11] "d+mePPxOMpadfnddOKOP2h14k/HCy23W03i1FXVetxAU+x4Zjsew+KMa2SrP52Lk"
## [12] "DQ4jvoqRMhGXjI5AOPVxuqhwNT0fgyG5EkI7HnzDzIOC6wMxRQHEEO4bgAXnbt5a"
## [13] "Uwk2RoECgYEA8hwPd8FmLmb1gr1zWvO4AZ0Lzd4v4XuIvIJ0wANScG6CJS9XafPV"
## [14] "zVPGhwjw8sv0t51CCoup2B85sOWIS2EDYv2Q44qm9Yr+Ns6nai317fVLaQr0XS8x"
## [15] "/ezgYnjFZS1G5E5jhAp7mK54pkJ9LipVFuAO8g369mCRQR6PW2yAjPkCgYEAyvAs"
## [16] "O8jqgMA1h0eEvWQ+D3peOAYwbVZuA4WsNlgMO3YEk9YzAYGvbgAn7X9Bc8mggAz0"
```

```
## [17] "6+CBV1DyUNQJkuajXyRxdpiPD1c8qgXAlZE6I15AAyG/nUcg7RhEQHd4HTLOmJ+Z"
## [18] "lqoTy7SuP82YnDPCT68JGvsnJWCmUQgL4m+smrcCgYBHhFBxYJitdk5pe0r6/+lH"
## [19] "2Lsm6c4c/h/LB4IzQgf1HD+nek+JBbUPPQL02ohKQEMehf5/HPhj1f11qqfTFGoq"
## [20] "sJo/DLL67z7es7ayX7c4vm+zLMA4Unui9XjmvaQZmgFJ6XnuBCa0WD1dZ2CQ5YJT"
## [21] "CoZ/q++JHcdqg/t21xs2CQKBgQCjyqr46dWTaw8JC4kwTxrj5TDsaNpnNQ4AG8B9"
## [22] "8ByXVU6mf4iVW7VaxBd10XLjYEYBc/Ot+XqLHdMlt62ueiY74S8OuFOm1ZMp6xCf"
## [23] "5yIUb7qcjH2aFFGX6zETExnH/zzN5GrTNpxZmo/VATx+PixDohNoSnMy8MnrtuHY"
## [24] "taeLCwKBgQDtBp9NCiG9u+2Eusvw1RKah7atf6kW9zlehSpJYXmOOcHOl3h7Dtp3"
## [25] "FqQw2CRWGdRoLKY3rOhyiZKVYqE9YXl7ICsbVEhT11myLoSaj65wG4en4yyYHrUV"
## [26] "+wfsoQgv9pW1vAZcUIghsCTiv8SRASO92xjXUNGNL9E/DtFVDyMH5g=="
## [27] "-----END RSA PRIVATE KEY-----"
```