ECE 571: Lab 4

> *Date: 2022-03-25*
>
> *Author: Zhaohui Yang*

The following results of 6 tasks are generated by 6 C programs (`task1.c` – `task6.c`), whose scheduling are integrated the attached script file `run_tasks.sh`. The `readme.md` file is a good description for attached files.

Task 1: Deriving the Private Key

For the private key$\langle d, n\rangle$, n is known. According to calculation procedure of RSA, d is `3587A24598E5F2A21DB007D89D18CC50ABA5075BA19A33890FE7C28A9B496AEB`

Task 2: Encrypting a Message

With the public key $\langle e, n\rangle$, the encrypted cipher:

`6FB078DA550B2650832661E14F4F8D2CFAEF475A0DF3A75CACDC5DE5CFC5FADC`

Task 3:Decrypting a Message

$C = M^e \bmod n$: `50617373776F72642069732064656573`

Task 4: Signing a Message

a. plaintext: `I owe you $2000.`

signature: `55A4E7F17F04CCFE2766E1EB32ADDBA890BBE92A6FBE2D785ED6E73CCB35E4CB`

b. plaintext: `I owe you $3000.`

signature: `BCC20FB7568E5D48E434C387C06A6025E90D29D848AF9C3EBAC0135D99305822`

It can be seen that although there is only 1-bit change in the plaintext sequence, the generated signatures differ in many bits. That is similar to the diffusion effect.

Task 5: Verifying a Signature

Origin message: `4C61756E63682061206D6973736C652E`
decrypted message from signature: `4C61756E63682061206D697373696C652E`

Comparing the origin message and decrypted message from signature with the private key $\langle d, n \rangle$, they are different. Thus the signature is not from Alice.

When the tail two-bit data are changed from `2F`1 to `3F`, the decrypted message is `91471927C80DF1E42C154FB4638CE8BC726D3D66C83A4EB6B7BE0203B41AC294`. The difference of the new decrypted message with the original message shows that "signature" techniques are very efficient and effective.

Task 6: Manually Verifying an X.509 Certificate

Herein I use the certification from `arizona.edu`, which is encrypted by RSA-256.

Step 1: download certification from the server

They are save into `ccc.txt`, `cc0.pem`, `cc1.pem`.

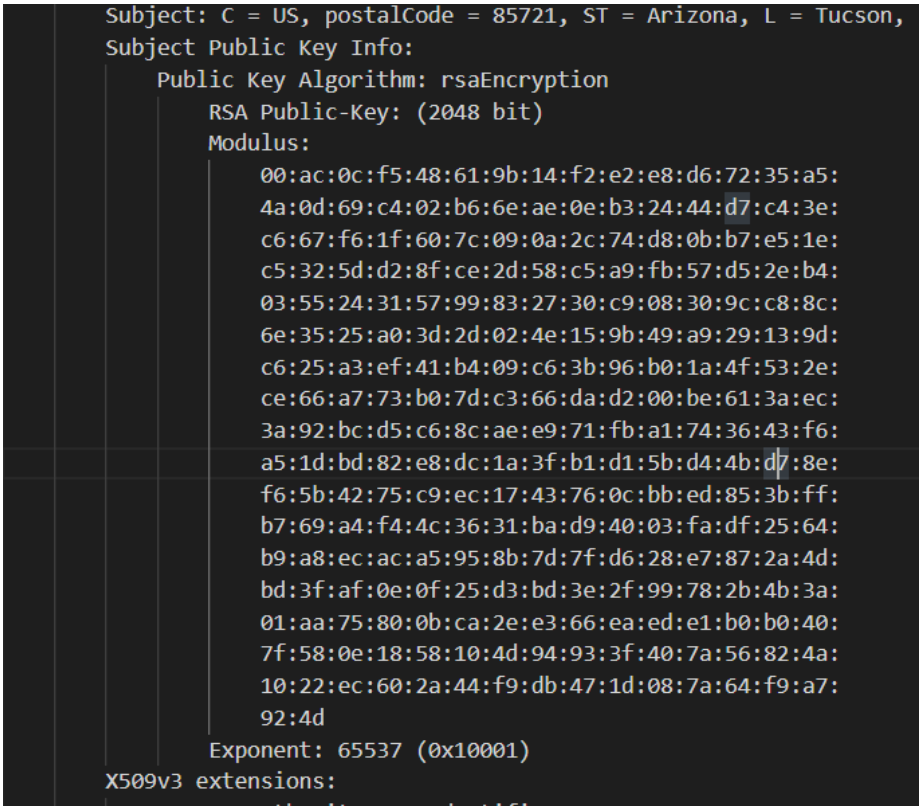
Step 2: extract $\langle e, n \rangle$

n:
`AC0CF548619B14F2E2E8D67235A54A0D69C402B66EAE0EB32444D7C43EC667F61F607C090A2C74D80BB7E51EC5325DD28FCE2D58C5A9FB57D52EB4035524315799832730C908309CC88C6E3525A03D2D024E159B49A929139DC625A3EF41B409C63B96B01A4F532ECE66A773B07DC366DAD200BE613AEC3A92BCD5C68CAEE971FBA1743643F6A51DBD82E8DC1A3FB1D15BD44BD78EF65B4275C9EC1743760CBBED853BFFB769A4F44C3631BAD94003FADF2564B9A8ECACA5958B7D7FD628E7872A4DBD3FAF0E0F25D3BD3E2F99782B4B3A01AA75800BCA2EE366EAEDE1B0B0407F580E1858104D94933F407A56824A1022EC602A44F9DB471D087A64F9A7924D`

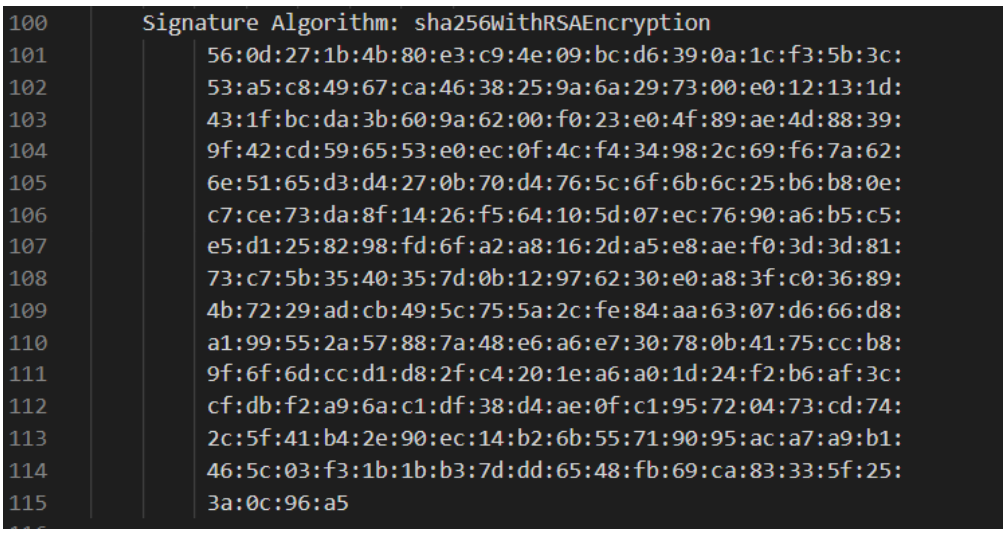
e: `10001` (hexadecimal)

```
(base) rose@DESKTOP-NS6V87H:~/Git-Projects/arizona-ece-course/INS/ins-lab-4$ openssl x509 -in cc0.pem -noout -modulus
Modulus=AC0CF548619B14F2E2E8D67235A54A0D69C402B66EAE0EB32444D7C43EC667F61F607C090A2C74D80BB7E51EC5325DD28FCE2D58C5A9FB57D52EB4035524315799832730C908309CC88C6E3525A03D2D024E159B49A929139DC625A3EF41B409C63B96B01A4F532ECE66A773B07DC366DAD200BE613AEC3A92BCD5C68CAEE971FBA1743643F6A51DBD82E8DC1A3FB1D15BD44BD78EF65B4275C9EC1743760CBBED853BFFB769A4F44C3631BAD94003FADF2564B9A8ECACA5958B7D7FD628E7872A4DBD3FAF0E0F25D3BD3E2F997822B4B3A01AA75800BCA2EE366EAEDE1B0B0407F580E1858104D94933F407A56824A1022EC602A44F9DB471D087A64F9A7924D
```

Both of them can be obtained from the detailed field data, by means of command `openssl x509 -in cc0.pem -text -noout` to extract.



Step 3: extract the signature



Step 4: extract the body of server's certification

It is in file `cc0_body.bin`.

Step 5: verify the certification

```
Task 6: Manually Verifying an X.509 Certificate
M_dec 419D0C8FED6BA6CDB771B6D64051F75101BE3CE2CB19C51D375E6A4DED832E54DF7562469557D437F0B094982F1D28CD7
9166A41354FC439E1A0865EE323C62FF2649FA4C1E581480C1A6D01D4867A79A897B1365F5933742728CA3CD6972024BC870D3E
C8C30392160A6DD713BC43391DAD777C4201D40B239BE76EE87E32A98AFA0249FD6AAA35C1A7D0015E4832FCC8D0973987DDDEB
D065AED9B054A1A51A1F329841F09BD395D8FBB418D8D7ECD38502B9331B3E2B1B5CEE3205260361F91F7876A58D3C71E5B1CC9
DE9DB4B67474F88F98C7B1396A6FE81FF54886B96840BB7F51E633BF79620C93445EFE46AF5FC198E2E21949D53E7A075C090EE
C86
correct hash for comparision:  30b8e177f6a24835fc21df98ac41a7a91d2ac4a5172f4ee5050f489e9412e79d
```