[수업]

prof) for compute\_pow(), use the pseudo code in hw4). You can't just keep multiplying or using pow() for compute\_pow() since it will not work for big numbers. Use the pseudo code provided in hw4). For "mod", you can use "%" operator.

= compue\_pow()는 강의노트 hw4)에 있는 코드를 사용하기 바랍니다. 숫자가 커지면 일반적인 pow() 함수 등으로는 계산을 할 수 없습니다. mod는 % 연산자를 사용하기 바랍니다.

[HOMEWORK]

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

RSA는 asymmetric 키 알고리즘을 사용합니다.

두 소수 p, q를 선택해, n=p\*q, phi1 = (p-1)\*(q-1), 를 구현합니다.  
만들어진 phi에서 phi와 서로소인 phi보다 작은 수 중에 하나를 선택합니다. =e.   
phi2는 phi1 보다 작은 수 중 phi1과 서로소인 수의 개수를 나타내고, 이렇게 구해진 phi2를 이용해 d=ephi2-**1mod** phi1 을 하여 구할 수 있습니다.   
: Public Key = (n, e) , Private Key = (n, d) 입니다.

5) Write a program that breaks your RSA system.

텍스트이(가) 표시된 사진

자동 생성된 설명

암호화시킨 C가 5이고 이를 복호화 시킨 Mp가 실제로 입력한 M과 같은 142임을 확인할 수 있습니다.

)Install openssl in your pc.

download openssl from http://gnuwin32.sourceforge.net/packages/openssl.htm

(get "complete package except source")

install in your pc

go to the installed directory/bin

double click on openssl (you may need to run as "administrator")

텍스트이(가) 표시된 사진

자동 생성된 설명

8-1) Generate an RSA key pair using openssl.

openssl> genrsa -out mykey.pem 1024

// generate public/private key pair in file "mykey.pem" with keysize 1024 bits.

// default size 512 bits if keysize is not specified

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

8-2) Convert mykey.pem to a text file, mykey.txt, to look at the contents. Use WordPad to open mykey.txt. Find n, e, and d.

openssl> rsa -in mykey.pem -text -out mykey.txt

// display the contents of "mykey.pem" in plain text in

// output file "mykey.txt"



텍스트이(가) 표시된 사진

자동 생성된 설명

modulus가 각 private, public key를 구성하는 요소 입니다.

publicExponent는 e, privateExponent는 d입니다. prime1은 p, prime2는 q를 의미합니다.

Exponent1은 d%(p-1), Exponent1 d%(q-1)입니다.   
coefficent는 inverse q에 mod p를 한 값입니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

8-3) Encrypt "hello" with (n, e) to produce ciphertext. What is the size of the ciphertext? Decrypt the ciphertext with (n, d) to recover "hello".

openssl> rsautl -encrypt -inkey mykey.pem -in myplain.txt -out mycipher // encrypting

openssl> rsautl -decrypt -inkey mykey.pem -in mycipher -out mycipher.dec // decrypting

Refer the manual in man/pdf/openssl-mal.pdf.

PEM(Privacy Enhanced Mail) file format transforms a binary file into an ascii file using base64. Each 6 bit in the input file will be converted to a letter in {A-Z, a-z, 0-9, +, -}, and wrapped with boundary lines.

ex) Man ==> 77 97 110 ==> 01001101 01100001 01101110

==> T(010011, 19) W(010110, 22) F(000101, 5) u(101110, 46)

(.der : binary DER encoded certificates

.cer : similar to .der

.key : PKCS#8 keys. the keys are encoded as binary DER or ASCII PEM)







mycipher 파일에 myplain.txt를 encrypt한 내용을 적게하였습니다.   
decrypt한 내용은 mycipher.dec에 넣었습니다.

myciper 내용은 다음과 같습니다.



dec 내용은 다음과 같습니다.



9) Make an X.509 certificate.

9.1) make a config file "myconf.txt"

[req]

string\_mask = nombstr

distinguished\_name = req\_distinguished\_name

prompt = no

[req\_distinguished\_name]

commonName = my CA

stateOrProvinceName = some state

countryName = US

emailAddress = root@somename.somewhere.com

organizationName = mycompany

텍스트이(가) 표시된 사진

자동 생성된 설명

= myconfig.txt file

9.2) Make a certificate for the person/company specified in myconf.txt. The public key of this person/company is given in mykey.pem:

req -config myconf.txt -new -x509 -key mykey.pem -out mycert.pem



앞서 만든 내용에 지정된 내용으로 인증서 파일을 mycert.pem 으로써 생성해줍니다.

텍스트이(가) 표시된 사진

자동 생성된 설명

9.3) let's read the contents of the certificate

x509 -in mycert.pem -text -out mycert.txt

Who is the owner of this certificate? What is the public key? What is the key size?

Who has signed this certificate?

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

인증서 공개키의 소유자는 my CA이고 인증서 발행기관은 my CA이빈다.   
공개키의 크기는 1024 bit이고 공개키의 값은 위와 같습니다.

10) Get a certificate in Internet Explorer or in Chrome. Check the contents of x.509 file.

10.1) Go to "tools>internet options>contents>certificates" to get a copy of a certificate. To view the certificate of a site:

In Chrome, go to some https site such as [www.daum.net](http://www.daum.net) and select Three Dots Menu>More Tools>Developer Tools>Security>View certificate>Details>Copy to File

In IE, go to some https site such as [www.daum.net](http://www.daum.net) and click the padlock symbol, select “View Certificate”>Detail>Copy to File.

10.2) Look at the contents of this certificate (assume the file name is daum.cer) with

x509 -in daum.cer -text -out daum.cer.txt -inform DER

Who is the owner of this certificate? Who has signed this certificate? What is the public key? What is the key size?

(DER: Distinguished Encoding Rules)