CTIS 496::Data Security in Computing::Fall 2012
Project / Announcement Date: 21.12.2012 /
Deadline: 14.01.2013, 16:00

NOTICES

1. **A group of at least two or at most three persons taking this course must do this project.**

2. **Copying someone else's solution to the project, or letting someone else copy your solution is strictly forbidden.**

3. **One compressed file containing project's report file, which covers questions answers, and source codes will be submitted as an attachment of e-mail sent to hmurat@bilkent.edu.tr** with subject: CTIS 496-Project / All Group members Name Surname

   Deadline: 14.01.2013, 16:00

4. **For the demo, each group should provide all necessary tools and environment (PC, software and IDE etc.) to run the demo after the Final Examination Date and before 14 January 2013, 16:00.**

5. **Printed copy of project's report file should be submitted.**

6. **All references being used should be clearly and correctly indicated in the reference part. Use your own words.**

7. **Your submitted project will be analyzed by "plagiarism detection program" "Turnitin" (visit http://library.bilkent.edu.tr/turnitin.html for its details).**

8. **During the project demo, there will be some questions about this project. If someone else submits his/her project regulary but s/he does not answer these questions correctly, then s/he will get zero (0) point from this project.**

SECTION I (100 pts) (S/MIME X.509 Certificates, E-mail Encryption and Signature, Use of GnuPGP, Use of Openssl)

(1) Each group member is required to use Mozilla Firefox (its version 1.5+) to get a free e-mail certificate from

http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html

Each group member will obtain this certificate within two or three days after starting the process. Using this certificate (X.509, S/MIME certificate), Each group member can digitally sign his/her email as well as encrypt his/her email messages by using Mozilla Thunderbird (free, open source, cross-platform e-mail and news client).

Important note: Use an e-mail address from the providers such as gmail.com or ug.bilkent.edu.tr supporting POP or IMAP service. If this is the case, then each group member should use "Mozilla Thunderbird" to read his/her e-mail messages and send e-mail messages and also encrypt or sign his/her e-mail messages.

After each member completes the last step required to get a a free e-mail

certificate from the above address, his/her certificate automatically loaded to Mozilla Firefox's certificate database. Use Mozilla Firefox and go to **Preferences > Advanced Tab > Encryption > View Certificates > Your Certificates** and select his/her name and click **"Backup"** button to backup his/her certificate into an external file (**name_surname.p12**). Here you need to provide his/her password to protect your p12 file that contains private key. Do not forget this password. Also click **"View"** button to find out the details of his/her certificate such as the name of the encryption algorithm, key length, issuer and hash algorithm.

Before load/install your certificate, on Mozilla Thunderbird, each member needs to create an account for his/her e-mail address and do necessary configurations for pop or imap settings.

In order to load/install his/her certificate into "Mozilla Thunderbird" , each member is required to carry out necessary steps (refer to "Installing an SMIME Certificate For Your Own Identity" part from the web page http://kb.mozillazine.org/Installing_an_SMIME_certificate).

As a group, mention experiences and ideas on that part. Write down the name of both the encryption algorithm and hash algorithm, key length, validity of each group member certificate, public key, serial number and issuer's common name, organization and organization unit.

How can one view the details of issuer' (Certificate Authorite of your certificate) certificate on Mozilla Thunderbird? Explain and describe your solution.

(2) Each group member should install OpenSSL on his/her system. Then using **openssl** command to obtain his/her public certificate that can be delivered to anyone using the p12 file created in Question **(1)**). The extension of this file should be pem (filename is **name_surname.pem**) and it can be obtained by using the following command

openssl pkcs12 -in name_surname.p12 -clcerts -nokeys -out name_surname.pem

Use OpenSSL to create digital signature (**name_surname.pem.signed)** of the file **name_surname.pem** using your private key available from the file **name_surname.p12** and use the hash function SHA-512.

Write down commands accomplishing that operation.

(3) Each group member is required to send files both **name_surname.pem** and **name_surname_pem.signed** to other group members.

Printed copy of project solutions should cover the contents of each group member certificate (such as http://www.bilkent.edu.tr/~hmurat/hmurat_yildirim.pem) .

Each member should check the integrity and autenticity of the file **name_surname.pem** (using the related openssl command, **name_surname_pem.signed** and necessary key and related cryptographic algorithms) that is received from the others.

Write down commands accomplishing that operation.

(4) Use Thunderbird (refer to "Other people's certificates" part from the web page

http://kb.mozillazine.org/Installing_an_SMIME_certificate) to load other group member Then each group member **(sender)** is required to send an encrypted and signed e-mail message to other group member **(receipt)** by using Mozilla Thunderbird (and both sender and receipt certificates). Each group member will verify the received message using certificates and decrypt it by using Thunderbird (and his/her private key).

Provide screen-shots for all operations performed between group members (For example, User A and User B & User B and User C if there are 3 group members) and discussed in this question such as encrypting, signing e-mail and verifying signed e-mail and decrypting encrypted e-mail.

(5) List **GnuPGP** commands and give all details in order to

a) create a key pair (public/private keys) for each group member;
b) register each public key with public keyservers;
c) find your project member's key on a public keyserver.
d) create a signature for a file that you determine.
e) verify signature created by one of your project members.

(6) List **openSSL** commands and give all details in order to encrypt the file you determine and the decrypt the corresponding encrypted file

a) by three block ciphers (each should use at least two block modes of operations) and two stream ciphers.
b) by RSA public key encryption algorithm.

SECTION II (Extra BONUS PART / 30 pts)

ANSWER ONLY TWO OF THE FOLLOWING QUESTIONS:

(1) Use OpenSSL Library (its wrapper for JAVA also available) or Bouncy Castle Library or any other free and open source crypto library to develop your application with GUI or command-line interface (CUI) supporting one or more than one of the following:

+ Key generation, encryption and decryption of given documents (using some symmetric encryption algorithms with different modes of operation),

+ Key generation, encryption and decryption of given documents (using some asymmetric encryption algorithms)

+ Generating hash value of given documents (using some hash algorithms).

(2) Use the command openssl to create (self-signed) SSL certificate for your domain name or your localhost. Then using this certificate, configure apache webserver to enable https connection for your web server. Finally, check whether this connection works properly or not. Note that during the demo, this test will be performed.

Describe all steps necessary to carry out that operation.

(3) Use “The GNU Multiple Precision Arithmetic Library (gmp)”,

+ write a C language program doing multiplication, addition, modular arithmetic and exponentiation for very large integers

+ write a C language program for generating very large prime numbers