CTIS 496::Computer and Network Security:: SPRING 2024-2025

Computer Technology and Information Systems, ID Bilkent University

SECOND HOMEWORK

Instructor: Hamdi Murat Yıldırım

Deadline (Strict): April 30, 2025, Wednesday 23:59

NOTICE TO THE STUDENTS

Read the instructions carefully listed below :

1) Two of you form a group and as a group you will be able submit your homework.
If only one student submit this homework, s/he will be able to consider
two e-mail addresses to answer Question 1 and Question 2.

2) Create a .docx or .odt file, provide the answers, and insert screenshots mentioned in Questions.
Then convert it into a pdf file.
Do not forget to write down name, surname and student ID of each member.

3) Each member should study, understand all questions and their answers.

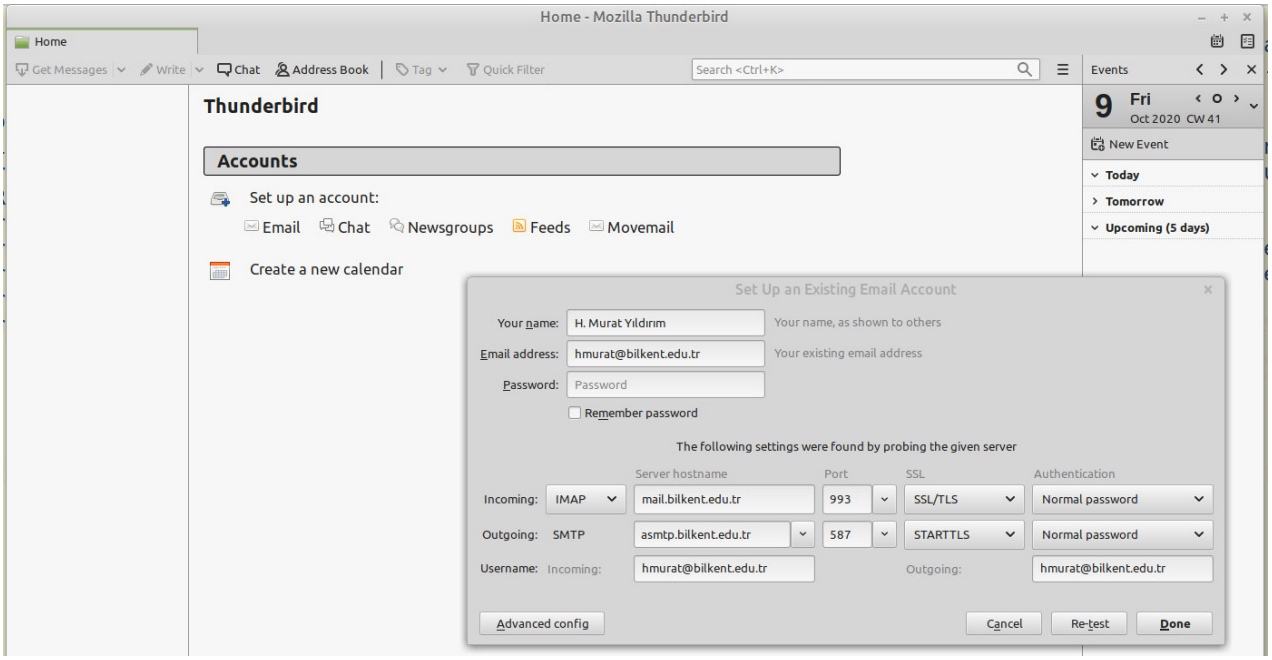
https://moodle.bilkent.edu.tr/2024-2025-spring/mod/assign/view.php?id=38143.

4) Copying someone else's or any other group solution to the homework,
or letting someone else copy your solution is strictly forbidden.

5) In CTIS 496 FINAL exam, there will be a set of questions about this homework.
If someone else submits his/her homework regularly but s/he does not answer these questions
correctly, then s/he will get zero (0) point from this homework.

Show all necessary steps while answering these questions in order to get full marks.

Refer the figure in the next page to configure your email account on Thunderbird.



IMPORTANT NOTE:
Download the lastest version of Thunderbird from (https://www.thunderbird.net/en-US/download/) ,and install it on your system.

QUESTION 1 **(20 pts)** Each group member is required to use Mozilla Firefox to get a free e-mail certificate from
`https://www.actalis.it/products/certificates-for-secure-electronic-mail.aspx`
`https://extrassl.actalis.it/portal/uapub/freemail?lang=en`

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 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 "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 > Privacy & Security > 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 Thunderbird, each member needs to create an account for his/her e-mail address and do necessary configurations for pop or imap settings (See the Figure in the second page). In order to load/install his/her certificate into "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. In that pdf file, provide the screenshot showing 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 Thunderbird? Explain and describe your solution.

QUESTION 2 **(35 pts)** 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
```

NOTE THAT each team member should provide screenshots showing the execution of this command.

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 decrypt the received message and verify its signature by using Thunderbird and all necessary keys.

Provide the screenshots showing all operations performed between group members (For example, User A and User B and discussed in this question such as encrypting, signing e-mail and verifying signed e-mail and decrypting encrypted e-mail.

QUESTION 3 **(15 pts)** You select any web server's which supports https. Replace **XXX** in the following command with *the domain name of this server.*

```
openssl s_client -showcerts  -connect XXX:443
```

Provide screenshots for this command and its output.
Describe what are included in the output of this command.

QUESTION 4 **(15 pts)** From a Trusted Third Party's online repository, download the CRL and display two certificates which were revoked (Hint: Operating System utility can be used to display it. You may use the openssl command to view it).
What is the last update's date and time?
What is the next update's date and time?

Provide screenshots for all steps of your answer, and mention about lessons you learned.

QUESTION 5 Solve either {part A) AND part B)} OR part C) of this question.
Provide screenshots for each step of the part you choose, and, mention about lessons you learned.

A) **(10 pts)** Choose a hostname or a full domain name, then create a self-signed X.509 certificate using the command openssl.

B) **(5 pts)** Using the command openssl, display the contents of the self-signed certificate created in part A).

C) **(25 pts -with BONUS-)** Alternative to part A) and part B), you can complete tasks in Section 1, Section 2, Section 3 (its first three subsections) of `https://seedsecuritylabs.org/Labs_20.04/Files/Crypto_PKI/Crypto_PKI.pdf` in order to get 10 points plus as BONUS. **LabSetup files: VM and Docker image files are available from** `https://seedsecuritylabs.org/labs.html`, and `https://seedsecuritylabs.org/Labs_20.04/Crypto/Crypto_PKI/`