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

Computer Technology and Information Systems, ID Bilkent University

FIRST HOMEWORK

Instructor: Hamdi Murat Yıldırım

Deadline: March 18, 2024, Tue, 13:00

NOTICE TO THE STUDENTS

Read the instructions carefully listed below :

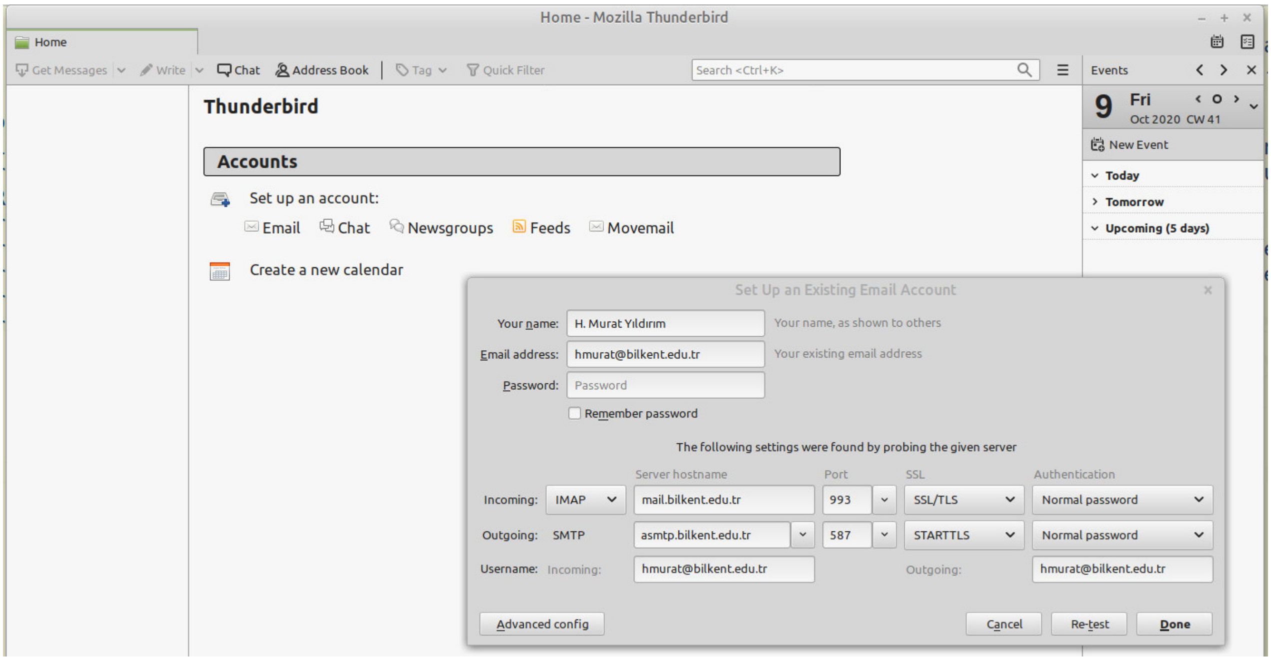
```
1) Two of you form a group and as a group you will be able submit your homework.
If only one student submit this homework, s/he will be able to consider
two e-mail addresses to answer the first question.

2) Create a .docx or .odt file, provide the answers, create TABLEs requested
and insert screenshots mentioned in Question 1) and 2). 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.

4) pdf file mentioned in 2) whose filename consists of surname of group members
(without using any blank character), e.g., surname1_surname2.pdf  will be submitted to
the course moodle web page:

https://moodle.bilkent.edu.tr/2024-2025-spring/mod/assign/view.php?id=30206.


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

6) In CTIS 496 MIDTERM 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.

QUESTION 1 IMPORTANT NOTE:

Download the lastest version of Thunderbird from (https://www.thunderbird.net/en-US/download/) ,and install gpg2, GNU PG for windows software -gpg4win- and https://gpgtools.org/ on Linux, Windows and MAC OS, respectively.

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



Set Up an Existing Email Account

Your name: H. Murat Yıldırım — Your name, as shown to others

Email address: hmurat@bilkent.edu.tr — Your existing email address

Password: Password

□ Remember password

The following settings were found by probing the given server

		Server hostname	Port	SSL	Authentication
Incoming:	IMAP	mail.bilkent.edu.tr	993	SSL/TLS	Normal password
Outgoing:	SMTP	asmtp.bilkent.edu.tr	587	STARTTLS	Normal password
Username:	Incoming:	hmurat@bilkent.edu.tr		Outgoing:	hmurat@bilkent.edu.tr

i) **(8 pts)** Each of you creates his/her PGP key pair for your e-mail (Algorithm RSA and its key size: 4096) AND *write down Key ID and fingerprint of each group member in a table (**TABLE 1**) with e-mail address in a pdf file.*

ii) **(8 pts)** Each of you uploads public key to public keyserver **http://pgp.circl.lu** and import other group members' public key from the keyserver **http://pgp.circl.lu**. *Display the contents of the public key ring on his/her system and take its screenshot which is provided in that pdf file.*

iii) **(8 pts)** Export the secret (private) key to a file using the command *gpg*. (Hint: See the lecture notes to learn how to make a key backup). Then import that secret key from this file in OpenPGP Key Manager of Thunderbird. *Screenshots showing that secret export and that secret import given in the pdf file.*

iv) **(10 pts)** Using **Thunderbird**, each of you sends both encrypted and signed e-mail to each of other two group members with subject *CTIS 496 FirstHW*. *Screenshots showing emails sent and emails received should be provided in that pdf file.*

v) **(10 pts)** Explain which PGP service used in part (iv) and what kind of security goals can be provided by using this service.

vi) **(10 pts)** For each of you, write all type of keys that s/he has used in part iv) and that other group member use to verify your signature and recover his/her message from the encrypted message
*in a table (**TABLE 2**) given in the pdf file.*

vii) **(6 pts)** For each of you, **all command(s)** necessary to encrypt a file using one of your group member's public key should be provided in a table (**TABLE 3**) (considering GNU pg, openpgp implementation) and *provide their screenshot in that pdf file.*

viii) **(6 pts)** For each of you, **all command(s)** necessary to decrypt the encrypted file in part vi) should be provided in a table (**TABLE 4**) (considering GNU pg, openpgp implementation) and *provide their screenshot in that pdf file.*

ix) **(6 pts)** For each of you, all command(s) necessary to digitally sign a file should be provided in a table (**TABLE 5**) (considering GNU pg, openpgp implementation) and *provide their screenshot in that pdf file.*

x) **(6 pts)** For each of you, **all command(s)** necessary to verify the signature of the file in part viii) should be provided in a table (**TABLE 6**) (considering GNU pg, openpgp implementation) and *provide their screenshot in that pdf file.*

xi) **(6 pts)** Each of you change the default trust level of other members' public key to Level 5. Re-run the commands in part x). Did you see any warning message? Why?

xii) **(6 pts)** Each of you digitally signs each of other group members' public key and upload this key to the public keyserver `http://pgp.circl.lu`. Each command executed by a group member is put in a table (**TABLE 7**). Use a web browser to browse the details of the public key from this server and *take its screenshot and provide it in that pdf file.*

QUESTION 2 **(10 pts)** Provide the URL of a software with its signature (different than any other group considers).
Download them and *show all necessary steps to verify this signature. Provide the screenshot for downloading them and verifying the signature in that pdf file.*
*That URL address and each command executed are put in a table (**TABLE 8**).*