Lab09 - Keys & Certificates

This week we will be working with public/private keys and X.509 certificates. We will learn how to generate RSA keys for use in SSH, view their specific parameters, and use them to encrypt, decrypt, and verify messages. We will also learn how to generate certificates, send them off to be signed by a certificate authority, and how to use them in signing and encrypting email messages. Instructions for submission are listed at the end of the document. All exercises will be performed on your Ubuntu18 desktop. **Note**: you'll need to perform all of the steps in order.

*all instances of <netid> should be replaced by **YOUR** netid:

```
vi <netid>_msg.txt         ⇒         vi luehm_msg.txt
```

Part 1

1. First, you will need to create a working directory to hold the documents generated during this homework. Create a new directory and change-directory into it:
   a. `mkdir lab09`
   b. `cd lab09`
2. Next, generate a public/private key pair on your machine using `openssl`. To generate the private key, execute the following command:
   a. `openssl genpkey -algorithm RSA -out <netid>_private_key.pem -pkeyopt rsa_keygen_bits:2048`
   b. This will generate a single file containing your private key in PEM format. You can `cat` the file to read the private key in base64
3. Extract your public key from the private key:
   a. `openssl rsa -pubout -in <netid>_private_key.pem -out <netid>_public_key.pem`
4. View all of your private key's data with:
   a. `openssl rsa -text -in <netid>_private_key.pem`
   b. This will show the modulus, exponents (public and private), primes (p and q) that were used to compute your key pair. It also shows exponents 1 and 2, as well as the coefficient, that are used in the Chinese Remainder Theorem which we didn't discuss in class. It is used during decryption with RSA because it is faster than exponentiation. **Submit a screenshot** of the output of this command.
   c. Generate one more key pair. **Comment on** what the various values mean in the textual output. 1) Which ones are constant throughout? 2) Which ones vary? 3) What do these values represent?
5. Use `ftp` to copy your public key to `certs.homework.331.com.` This will allow auto-magically generated messages to be signed with your public key.

a. From within the directory you created your public/private key pairs, enter the command: `ftp`
b. Type: `open certs.homework.331.com` and hit enter
c. Enter username and password: `anonymous` and hit enter
d. Change directory to `upload_rsa_keys` with the following command:
   i. `cd upload_rsa_keys`
e. Type: `put <netid>_public_key.pem` to upload your public key.
f. **Please note:** The key you upload should be in your current working directory and in the following format (should be if you've been following the instructions so far):
   i. <netid>_public_key.pem
g. Close connection with `close` and `quit`
h. If you need to re-upload a file, you can delete your public key (while logged in as anonymous) with the following command:
   i. `delete <netid>_public_key.pem`

6. The server should automatically add your public key to the `authorized_keys` file for the `ssh_guest` user. We can now use SSH and its supported tools (SFTP, rsync) to retrieve/put files on our server.
   a. Change the permissions on your private key: `chmod 600 <netid>_private_key.pem`
   b. Type the following command to open a sftp session. We will be connecting via a shared account to retrieve our messages.
      i. `sftp -i <netid>_private_key.pem ssh_guest@certs.homework.331.com`
      ii. You may be faced with a message about the authenticity of the host - just follow the on-screen instructions. Should only happen the first time connecting.
   c. Once connected, cd into your "messages" directory
      i. `cd lab09/rsa_msgs`
   d. Copy your "messages" directory to your machine:
      i. `get -r <netid>`
   e. Exit the session via: `exit`
   f. This should recursively copy a directory containing five automatically generated messages, the Certificate Authority's public certificate and "my" public certificate to your virtual desktop. There is also a signature file "sig.txt.sha256" that will allow you to test the authenticity of each of the messages.
   g. Copy the cacert.pem and the lab09_public_key.pem files to your lab09 directory on your 331 VM to make finding them easier for future steps (keep the ".." at the end of the commands).
      i. `cd <netid>`
      ii. `cp lab09_public_key.pem ..`
      iii. `cp cacert.pem ..`

   h. Google the differences between FTP and SFTP. **<u>Answer the following questions</u>**: 1) Why would you want one over the other? 2) Why did we need to specify our private key? 3) What protection does this offer?

7. Use the following command to verify each of your five messages
   a. `openssl dgst -sha256 -verify` **`lab09_public_key.pem`** `-signature sig.txt.sha256 <filename>.txt`
   b. This command compares the hash of the specified message against the provided signature. Four messages have been "modified" and one is the true message. Determine which message has not been modified and include **a screenshot** in your homework submission.
   c. **<u>Comment on</u>** what you've just done by explaining what the openssl command is doing and why this is significant. 1) What is known about the message? 2) What is the message protected against and what is it vulnerable to?
8. Now you will generate your own message and encrypt it.
   a. Change directory back to your lab09 folder: `cd ~/lab09`
   b. Using your favorite text editor (nano, vim, Text Editor, etc…) create a plain-text message and save it to your lab09 directory as `plain.txt`
   c. Encrypt the message using the provided public key as follows:
      i. `openssl rsautl -encrypt -inkey` **`lab09_public_key.pem`** `-pubin -in plain.txt -out <netid>_encrypt.dat`
   d. Using SFTP, upload this file to the certs server
      i. `sftp -i <netid>_private_key.pem ssh_guest@certs.homework.331.com`
      ii. `cd lab09/encrypted_msgs`
      iii. `put <netid>_encrypt.dat`
      iv. `exit`
   e. **Comment on** what this message is protected against and what it is vulnerable to (compared to the message we downloaded in step 6).
9. Generate a X.509 certificate signing request to be submitted using your RSA private key
   a. Ensure that you are in your lab09 folder: `cd ~/lab09`
   b. `openssl req -new -key <netid>_private_key.pem -out <netid>_certificate.csr -days 3650`
   c. You should be prompted to answer a series of questions. Ensure that you answer these as follows:

i.	<u>Country Name</u>:	US
ii.	<u>State or Province Name:</u>	Iowa
iii.	<u>Locality Name</u>:	Ames
iv.	<u>Organization Name:</u>	331.com
v.	<u>Organizational Unit Name:</u>	homework
vi.	<u>Common Name</u>:	<netid>.homework.331.com
vii.	<u>Email Address:</u>	<netid>@homework.331.com

   d. Ensure that you **do not** enter a challenge password or optional company name. Just press “Enter” when presented with these fields. If you mess up, you can always cancel with “Ctrl+C”

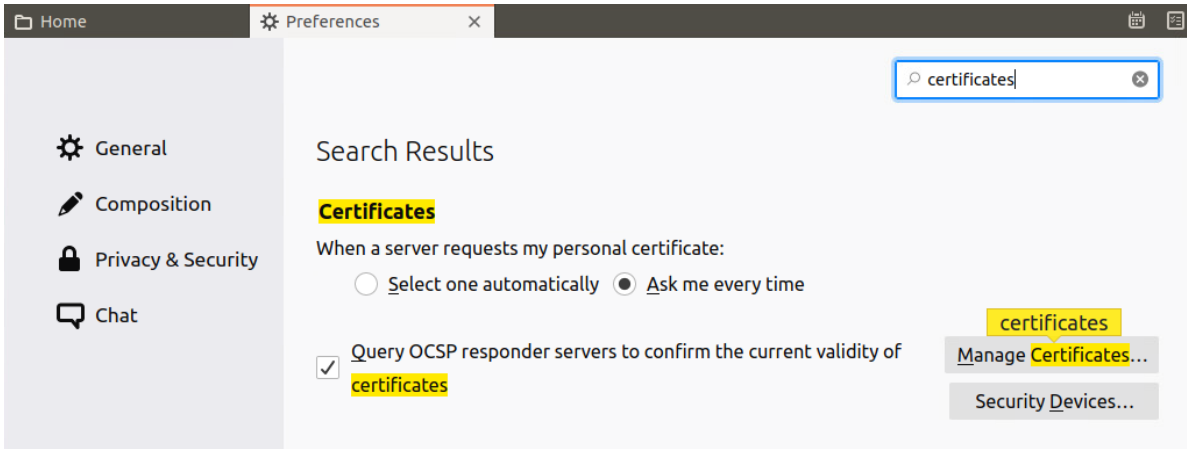
10. Upload your CSR to be signed, similar to uploading your public key earlier
    a. Start the interactive FTP program: `ftp`
    b. Open a connection: `open certs.homework.331.com`
    c. Log in as: `anonymous`
    d. Change directory to: `upload_cert_req`
    e. Upload your CSR: `put <netid>_certificate.csr`
    f. Note: you won’t be able to do this twice, so if you make a mistake and have to do it over, reach out to the TA so they can remove you from the certificate database.
11. Retrieve your signed certificate
    a. While still logged into FTP, change directory to: `download_cert` via the command:
       i. `cd ../download_cert`
    b. Retrieve your certificate with: `get <netid>_certificate.pem`
    c. Close connection: `close; quit;`
12. View your certificate
    a. Run the following command to view the contents of your newly signed certificate:
    b. `openssl x509 -in <netid>_certificate.pem -text -noout`
    c. **Include** screenshots of the output
    d. Do any parts of the certificate match with your private key? If so, why?
    e. What was happening during the Certificate Signing process? Why did you need to submit it for signing?
13. Create a signing certificate with the command:
    a.
    ```
    openssl pkcs12 -export -out <netid>_certificate.pfx -inkey
    <netid>_private_key.pem -in <netid>_certificate.pem
    -certfile cacert.pem
    ```
    b. When asked for a password, just hit enter for a blank password.
    c. This certificate will allow you to cryptographically sign a message.

Part 2

Configure Thunderbird

   a. Open Thunderbird.
   b. First we must configure Thunderbird to use our Certificate Authority's public certificate. This will allow your desktop to trust the email server’s identity and allow us to use our Certificate Authority’s certificates without constant warnings.
   c. Close the popup prompt asking to create/use an existing email account (will only happen the first time you run Thunderbird).
   d. From the menu at the top right corner of the screen, select “Settings”

e. In the search bar, type “certificates”, and click the “Manage Certificates” button.



Search Results

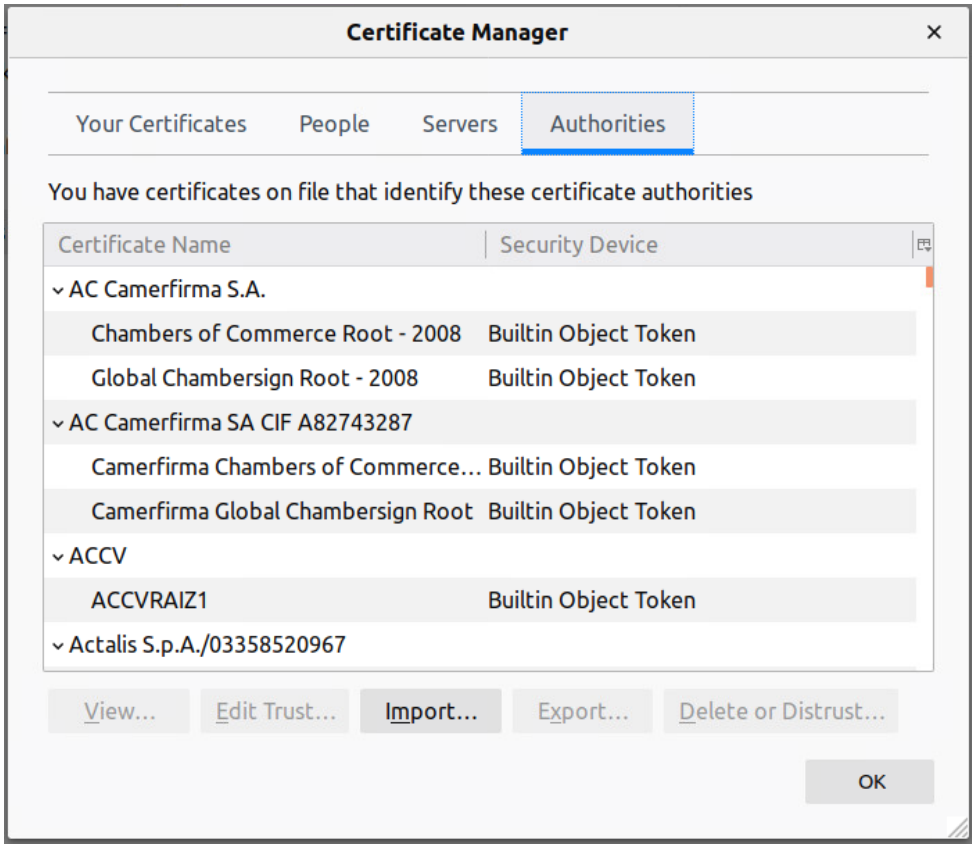
Certificates

When a server requests my personal certificate:

Select one automatically [✓ Ask me every time]

[✓] Query OCSP responder servers to confirm the current validity of certificates

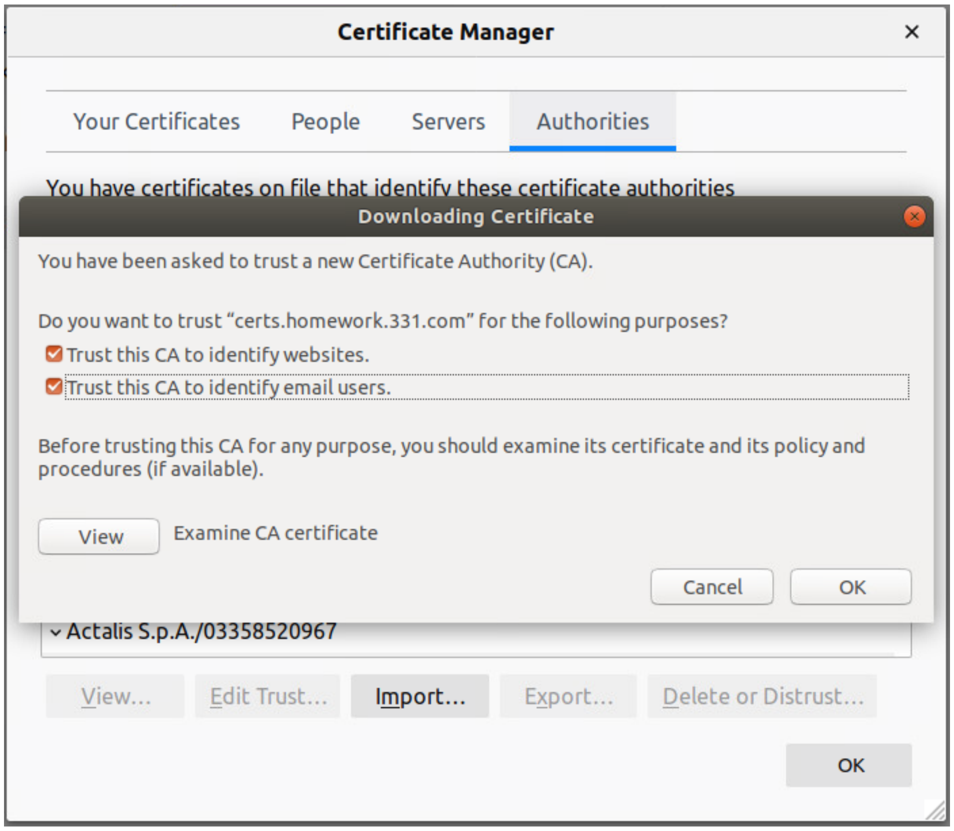
f. Ensure that the “Authorities” tab has been selected, then click the “Import” button.


Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce…	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token
⌄ Actalis S.p.A./03358520967	

g. Select the certificate `cacert.pem` certificate that was included in your message download in step 5. Check the boxes that allow the certificate to be used to identify websites and email users.

h. 

Certificate Manager

Your Certificates | People | Servers | Authorities

You have certificates on file that identify these certificate authorities

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "certs.homework.331.com" for the following purposes?

- [✓] Trust this CA to identify websites.
- [✓] Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View | Examine CA certificate

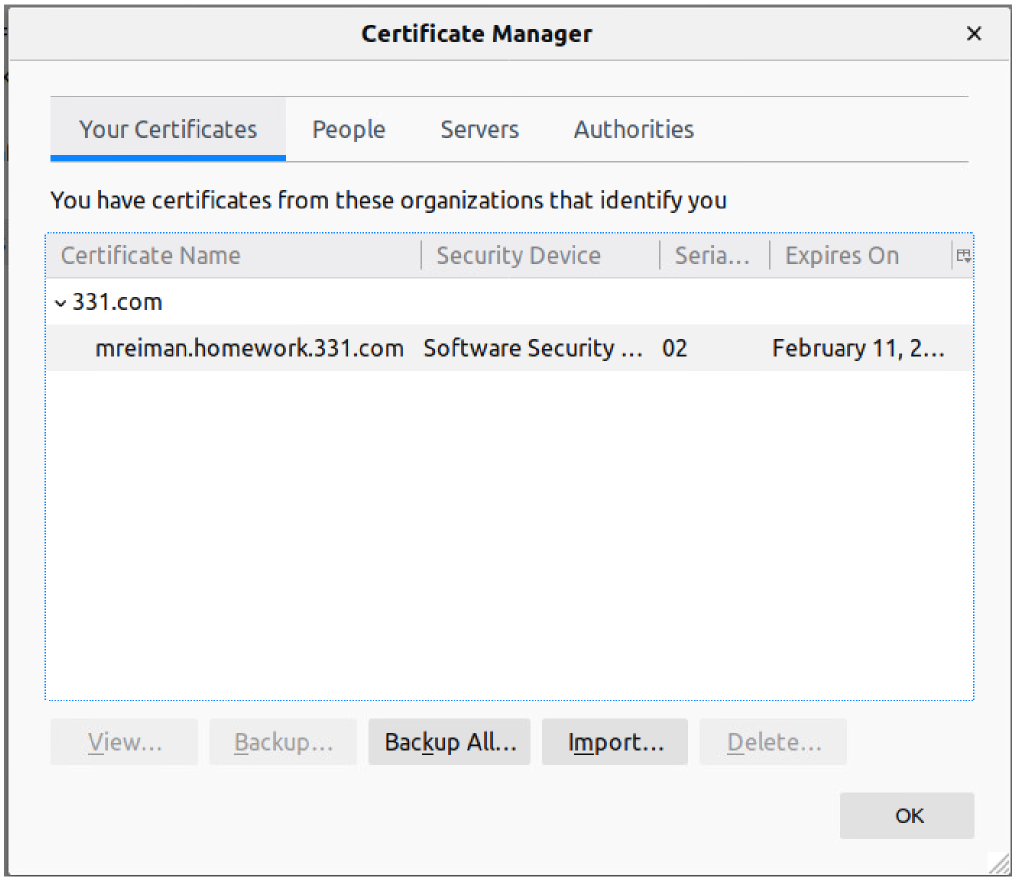
Cancel | OK

Actalis S.p.A./03358520967

View... | Edit Trust... | Import... | Export... | Delete or Distrust...

OK

i. Next, select the "Your Certificates" tab and import the certificate you created in step 13. When asked for a password, just continue with an empty password.


Certificate Manager

You have certificates from these organizations that identify you

Certificate Name	Security Device	Seria...	Expires On
331.com			
mreiman.homework.331.com	Software Security ...	02	February 11, 2...

j.

k. Close out of the Certificate Manager and the Preferences pane.

l. From the menu at the top right corner of the screen, select “Account Settings”

m. Near the bottom left of the window, select “Account Actions -> Add Mail Account”

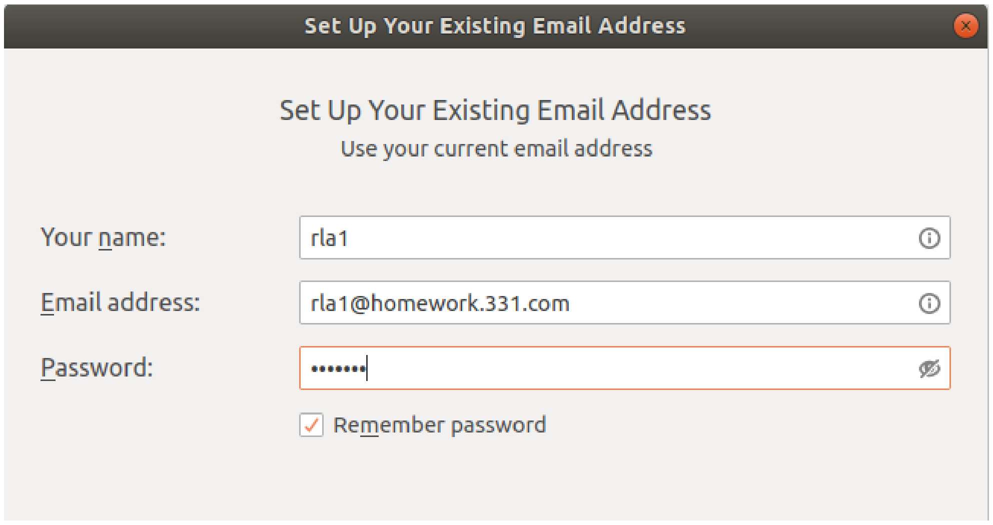
n. In the Setup window, enter:

   i. Enter your name: `<netid>`

   ii. Enter email address: `<netid>@homework.331.com`

   iii. Enter password: `cpre331`

o. Click continue

p. 
Set Up Your Existing Email Address

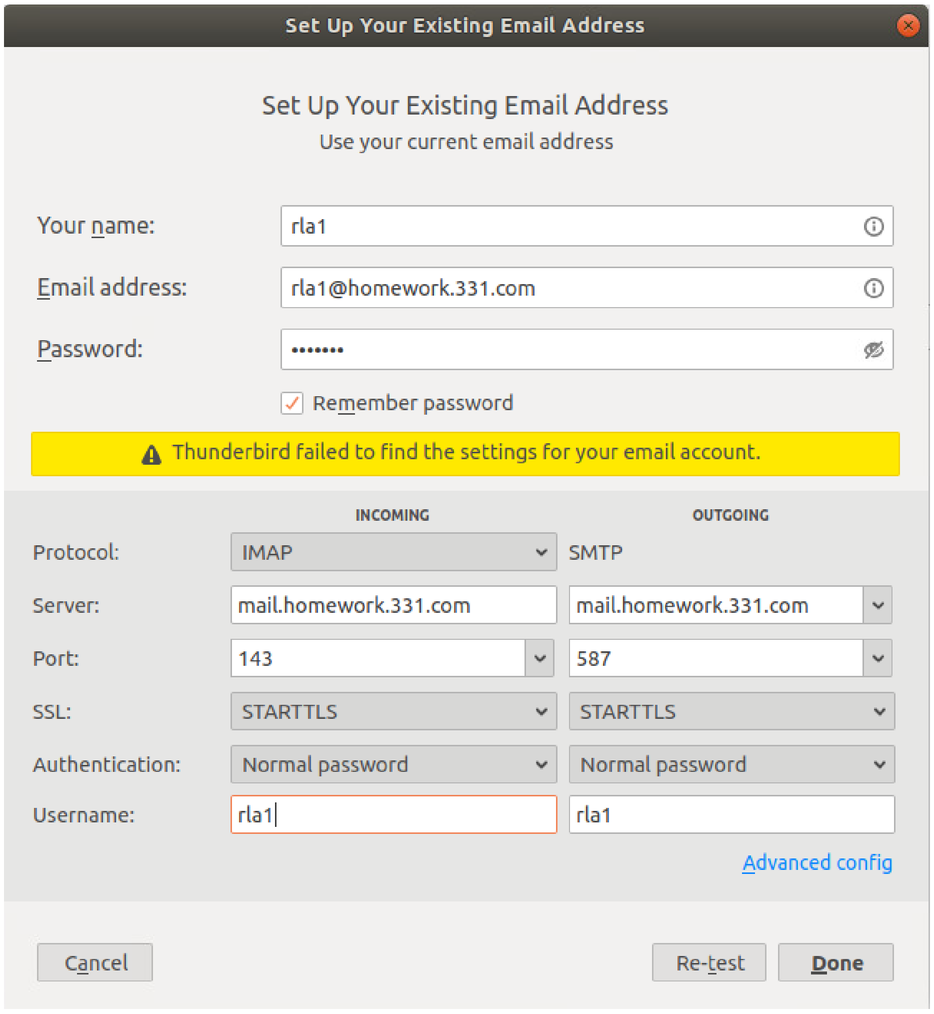
Set Up Your Existing Email Address
Use your current email address

Your name:	rla1
Email address:	rla1@homework.331.com
Password:	•••••••

✓ Remember password

q. Click Continue

r. If Thunderbird is unable to find the setting for your email account, match your setting to the image below (use your own netid and email) and click Done.

s. 
Set Up Your Existing Email Address

Set Up Your Existing Email Address
Use your current email address

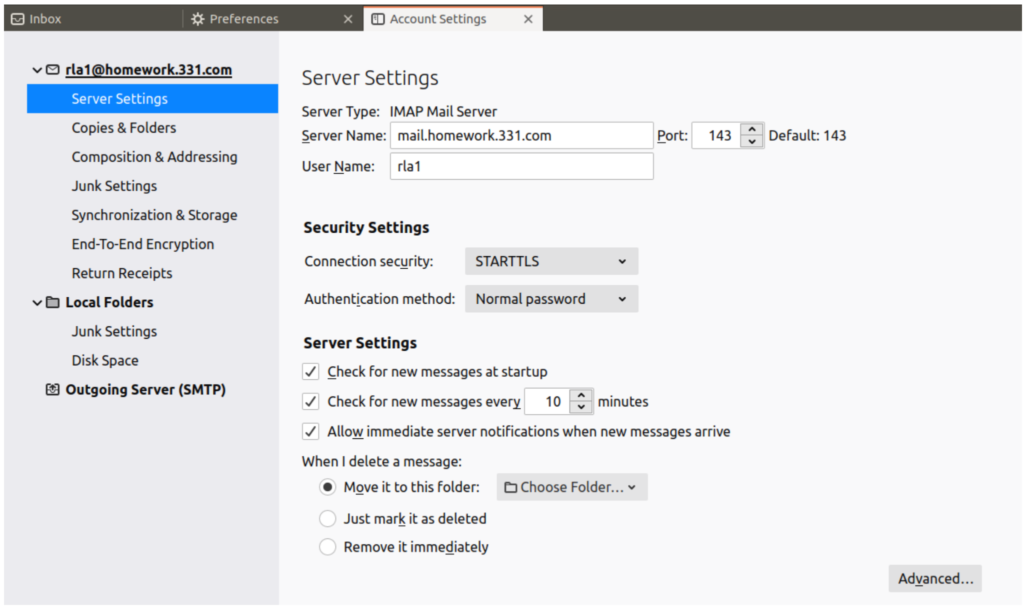
Your name:	rla1
Email address:	rla1@homework.331.com
Password:	•••••••

✓ Remember password

Thunderbird failed to find the settings for your email account.

	INCOMING	OUTGOING
Protocol:	IMAP	SMTP
Server:	mail.homework.331.com	mail.homework.331.com
Port:	143	587
SSL:	STARTTLS	STARTTLS
Authentication:	Normal password	Normal password
Username:	rla1	rla1

t. Change and click “Done” again. If that still does not work, click “Advanced Config”. You will be brought back to the account settings page.
u. First, configure the incoming mail server to look like the screenshot below.

v. 

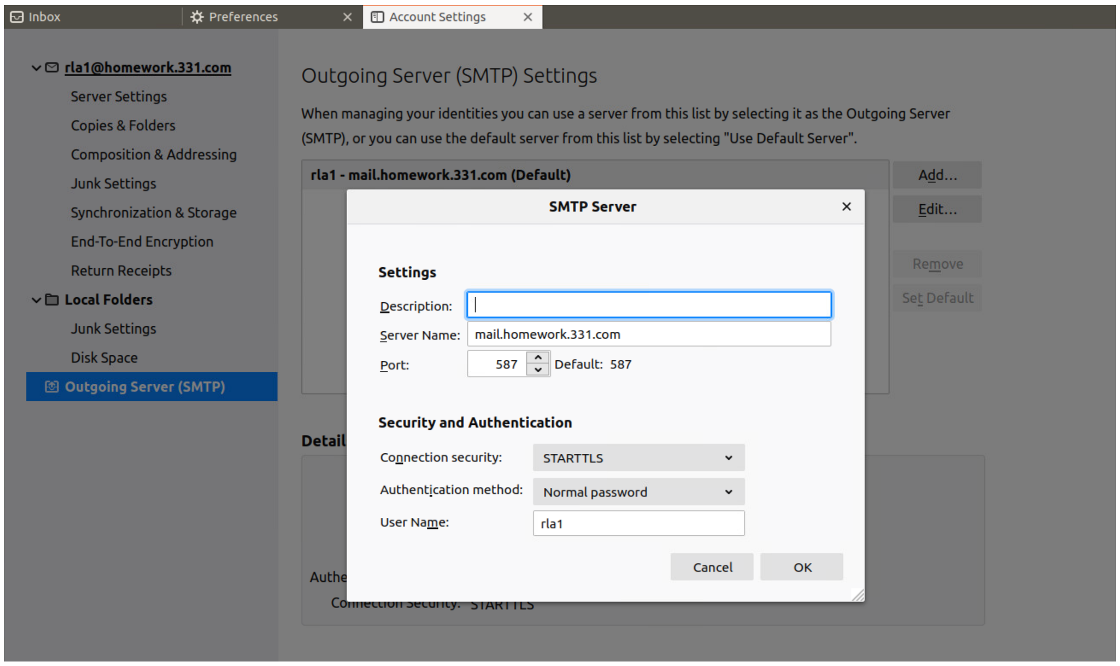
Server Settings

Server Type: IMAP Mail Server
Server Name: mail.homework.331.com Port: 143 Default: 143
User Name: rla1

Security Settings
Connection security: STARTTLS
Authentication method: Normal password

Server Settings
✓ Check for new messages at startup
✓ Check for new messages every 10 minutes
✓ Allow immediate server notifications when new messages arrive
When I delete a message:
● Move it to this folder:
○ Just mark it as deleted
○ Remove it immediately

w. Next, to configure the Outgoing server, select “Outgoing server” on the left hand side, and configure the outgoing server to look like the one below. Be sure to select “Edit”

x. 

Outgoing Server (SMTP) Settings

When managing your identities you can use a server from this list by selecting it as the Outgoing Server (SMTP), or you can use the default server from this list by selecting "Use Default Server".

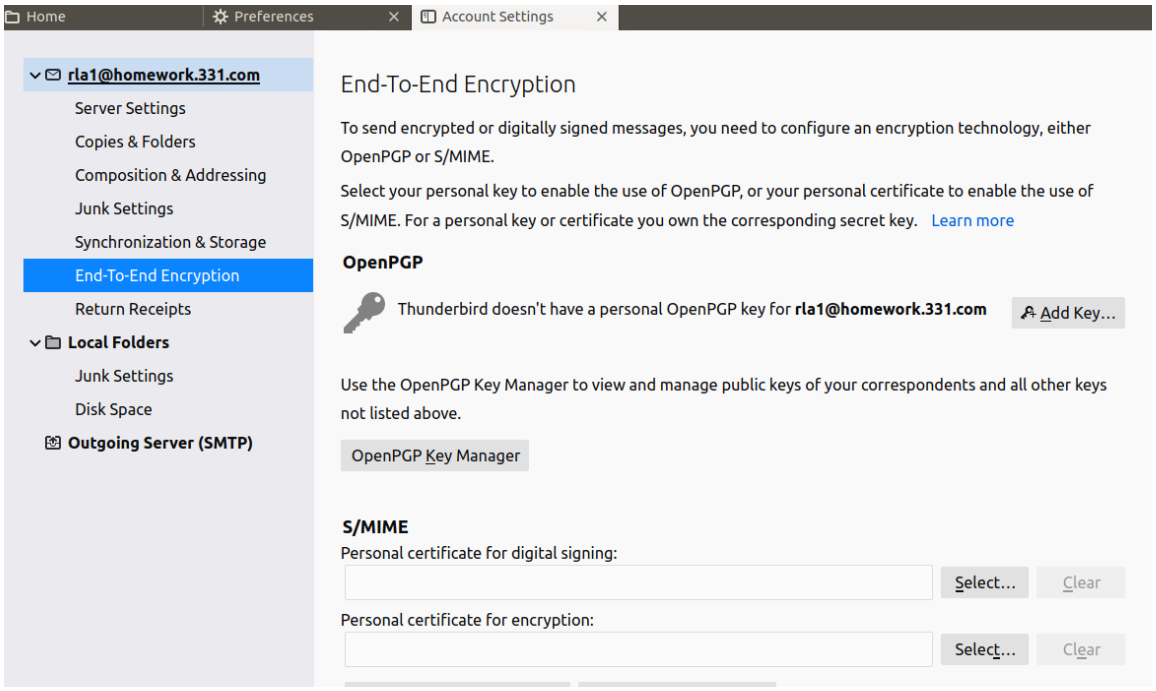
rla1 - mail.homework.331.com (Default)

SMTP Server

Settings
Description:
Server Name: mail.homework.331.com
Port: 587 Default: 587

Security and Authentication
Connection security: STARTTLS
Authentication method: Normal password
User Name: rla1

Install signing certificate into Thunderbird
y. Navigate to “Account Settings” (should still be open, else “Menu in the top write -> Account Settings”)
z. Select “End-To-End Encryption”, under “S/MIME” click “Select”



End-To-End Encryption

To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME.

Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more

OpenPGP

Thunderbird doesn't have a personal OpenPGP key for **rla1@homework.331.com**

Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above.

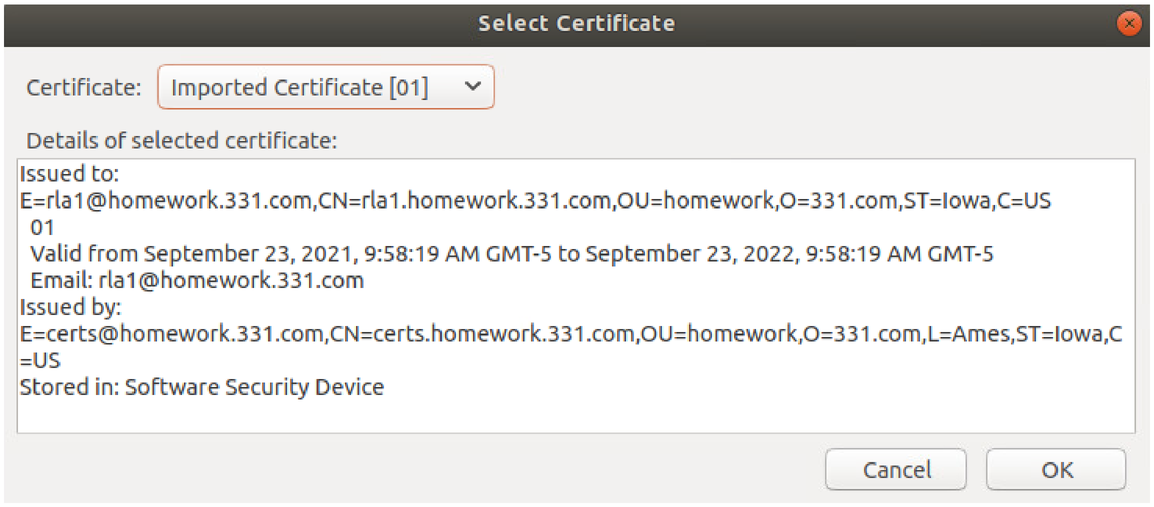
S/MIME

Personal certificate for digital signing:

Personal certificate for encryption:

aa.

bb. Select your imported certificate.



Select Certificate

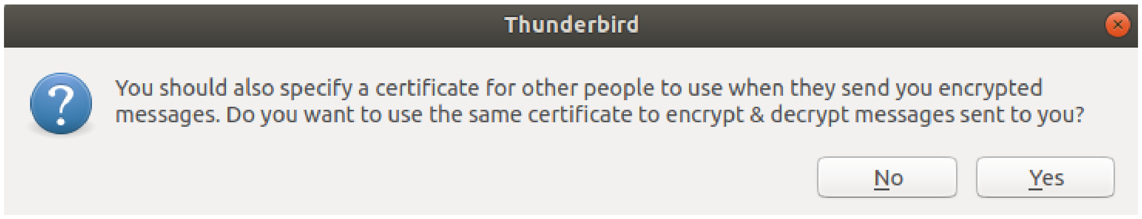
Certificate: Imported Certificate [01]

Details of selected certificate:

Issued to:
E=rla1@homework.331.com,CN=rla1.homework.331.com,OU=homework,O=331.com,ST=Iowa,C=US
01
Valid from September 23, 2021, 9:58:19 AM GMT-5 to September 23, 2022, 9:58:19 AM GMT-5
Email: rla1@homework.331.com
Issued by:
E=certs@homework.331.com,CN=certs.homework.331.com,OU=homework,O=331.com,L=Ames,ST=Iowa,C=US
Stored in: Software Security Device

cc.

dd. Click yes to the box asking if you should use the same certificate for encryption/decryption.



Thunderbird

You should also specify a certificate for other people to use when they send you encrypted messages. Do you want to use the same certificate to encrypt & decrypt messages sent to you?

ee.

Write an email to a fellow classmate, signing and encrypting it with your certificate.

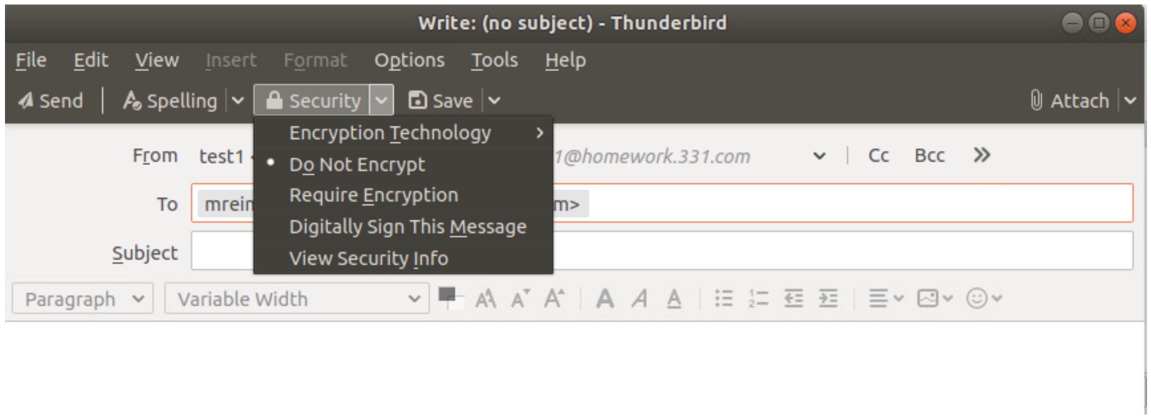
ff. Thunderbird automatically adds any certificate attached to an incoming email to your certificate manager. This reduces much confusion in certificate management. At first, you will only have your own certificate, so you will only be able to send signed messages. However, after receiving a message, you will be able to send signed and encrypted messages between yourselves. Therefore you are to:

i. Send a signed message to a classmate
ii. They are to respond with signed and encrypted message.
iii. You are then to respond with a signed and encrypted message of your own.

gg. To compose a new message, click the icon to compose a new message, or select "New Message" from the File menu.

hh. Type in the email of the person you wish to send a message to, in the format of "<netid>@homework.331.com".

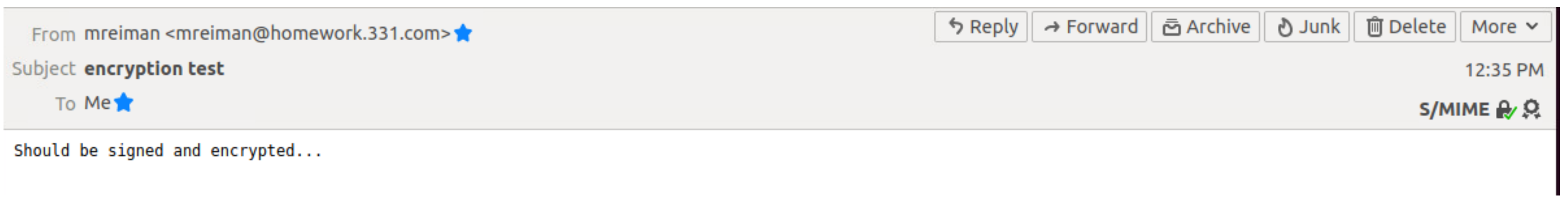
ii. You can modify the security settings of an email during composition via the "Security" menu near the top of the Write: pane. Depending on which state you are at in the message exchange, you will either select to only "Digitally Sign This Message" or will select both options (by accessing the menu twice) to "Digitally Sign" and "Require Encryption"



jj.

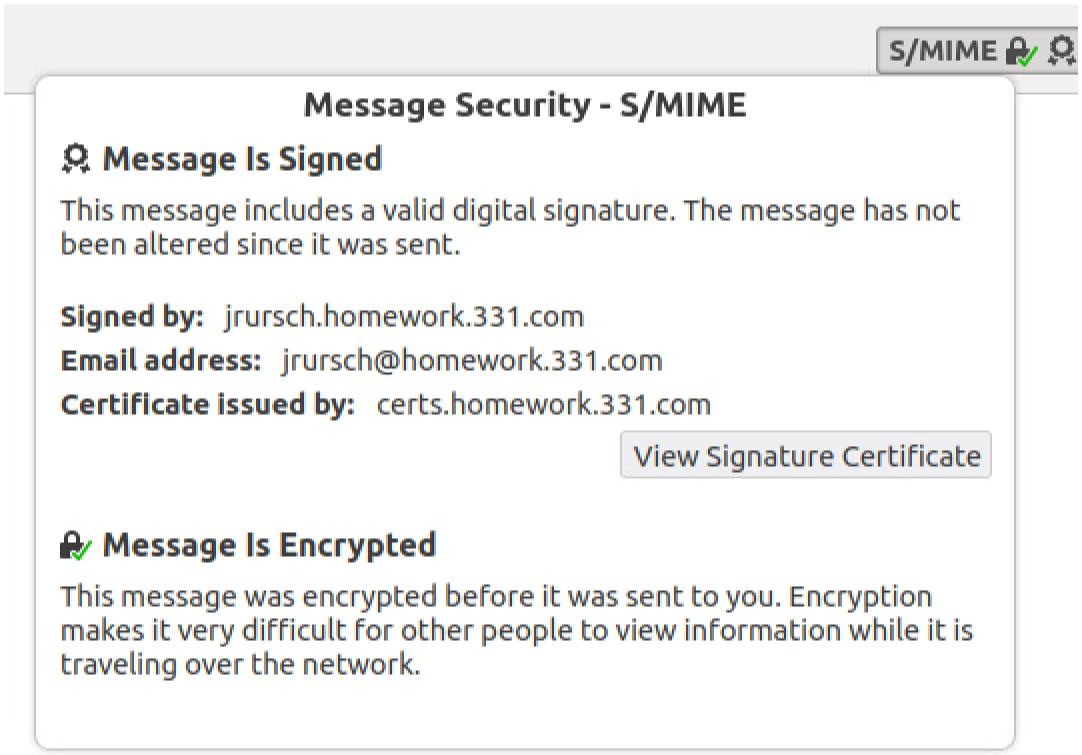
kk. After selecting your security option and filling out the Subject and Body of your message, click "Send" to send it on its way.

ll. After performing the three steps (signed, signed&encrypted, signed&encrypted) both parties should have a message like below, displaying both icons for signed (S/MIME and ribbon) and encrypted (padlock with checkmark). **Include a screenshot** of the resulting message.



From mreiman <mreiman@homework.331.com>
Subject **encryption test**
To Me
12:35 PM

```
Should be signed and encrypted...
```


S/MIME

Message Security - S/MIME

Message Is Signed

This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: jrursch.homework.331.com
Email address: jrursch@homework.331.com
Certificate issued by: certs.homework.331.com

Message Is Encrypted

This message was encrypted before it was sent to you. Encryption makes it very difficult for other people to view information while it is traveling over the network.

mm. If you need somebody to send messages with, you can find willing classmates on the slack channel.

nn. **Explain** why you couldn't send an encrypted message straight away - why did you need to send a signed-only message first?

Lab 05 Template

Some questions require multiple parts to be answered, be sure to discuss them in full.

1) Part 1:
   a. **Screenshot of the output from** `openssl rsa -text -in <netid>_private_key.pem`
      (10 points)

   b. **Comparison of the same/different values observed across the extra generated keys**
      i. Which values are constant?
      ii. Which ones vary?
      iii. What do these values represent?

      (10 points)

   c. **Discussion of the differences between FTP and SFTP.**
      i. Why would you want one over the other?
      ii. Why did we need to specify our private key?
      iii. What protection does this offer?

      (10 points)

   d. **Screenshot of the five messages [netid]1.txt, [netid]2.txt, … [netid]5.txt**
      (10 points)

   e. **Discussion on hash verification**
      i. What is known about the message?
      ii. What is the message protected against and what is it vulnerable to?

      (10 points)

   f. **Discussion on what the message generated in step 8e protected against and what it is vulnerable to (compared to the message we downloaded in step 6).**
      (10 points)

   g. **Screenshot of the signed certificate ([netid]_certificate.pem) when looked at through openssl**
      (10 points)

   h. **Discussion from step 12**
      i. **Do any parts of the certificate match with your private key? If so, why?**

ii. **What was happening during the Certificate Signing process? Why did you need to submit it for signing?**
(10 points)

2) Part 2:
   a. **Screenshot of signed and encrypted message received from a classmate**
   (10 points)

   b. Explain why you couldn't send an encrypted message straight away - why did you need to send a signed-only message first?
   (10 points)