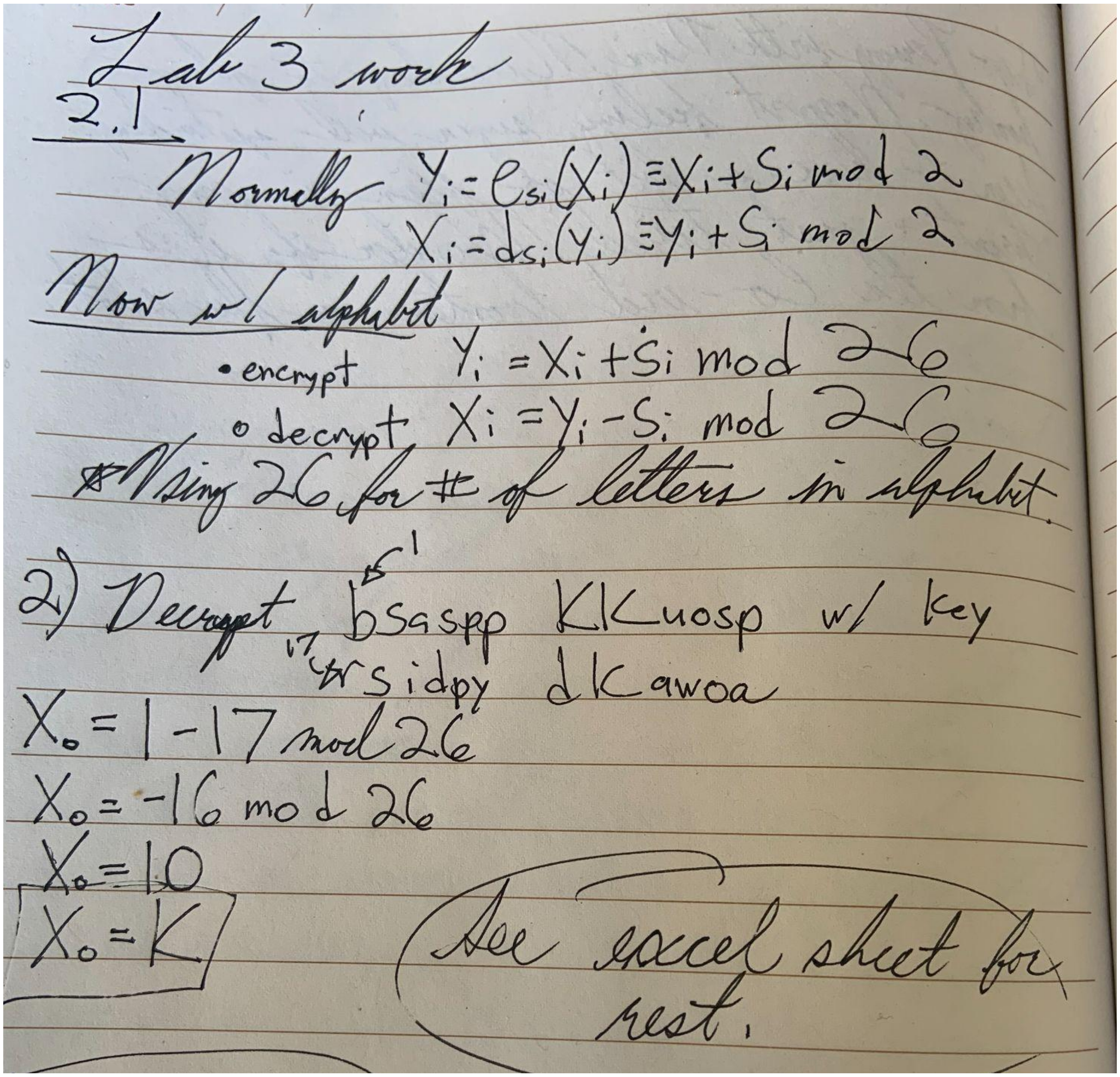
Carl Cortez

CIS 628

Chapter 2

Lab 3

2.1



Lab 3 work

2.1

Normally $Y_i = e_{s_i}(X_i) \equiv X_i + S_i \bmod 2$

$X_i = d_{s_i}(Y_i) \equiv Y_i + S_i \bmod 2$

Now w/ alphabet

- encrypt $Y_i = X_i + S_i \bmod 26$
- decrypt $X_i = Y_i - S_i \bmod 26$

*Using 26 for # of letters in alphabet.

2) Decrypt $\overset{1}{\text{b}}$saspp KKuosp w/ key $\overset{17}{\text{r}}$sidpy dKawoa

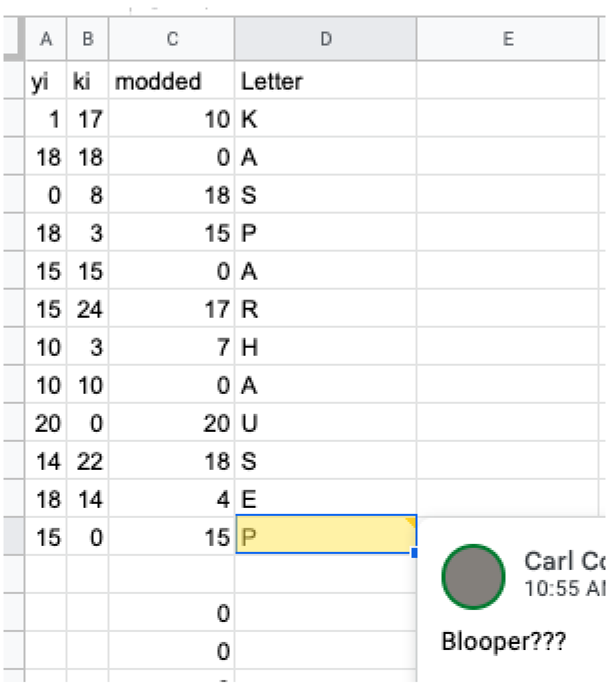
$X_0 = 1 - 17 \bmod 26$

$X_0 = -16 \bmod 26$

$X_0 = 10$

$\boxed{X_0 = K}$

See excel sheet for rest.



yi	ki	modded	Letter
1	17	10	K
18	18	0	A
0	8	18	S
18	3	15	P
15	15	0	A
15	24	17	R
10	3	7	H
10	10	0	A
20	0	20	U
14	22	18	S
18	14	4	E
15	0	15	P
		0	
		0	

Carl C
10:55 A

Blooper???

Excel sheet for work on task 2

Assuming there is a blooper, the decrypted message should be Kaspar Hauser.

Task 3) Kaspar was murdered by a stab to his left breast. What a shame!

2.2

The first thing that would worry me about this key is how data can be recovered if the disc is scratched or melted. Also with theft, it would be a shame if the CD fell into the wrong hands. From the definition, the key stream *should* only be known by the legitimate communicating parties. If a robbery occurred and the CD went missing, this could throw the communication line off. A possibility from this robbery is that the key gets copied.

For the life cycle of the key, if CDs become obsolete, it may be a challenge to read the CD. We're already seeing DVDs and physical copies of data dwindle down in production. Assuming our recipient is trustworthy, we should hope that they also destroy the CD in a timely fashion. Continuing to make sure that none of the data has slipped through or been leaked to another location.

In case there is a program that can revive one time keys, the CD should be stored indefinitely by the sender and recipient. Since using this CD once will jeopardize the key, we shouldn't reuse the key to encrypt other data; one and done. Our sizing of the cipher and plaintext should match the capacity of the CD-ROM; exactly 1 GByte.

<u>2.3</u>

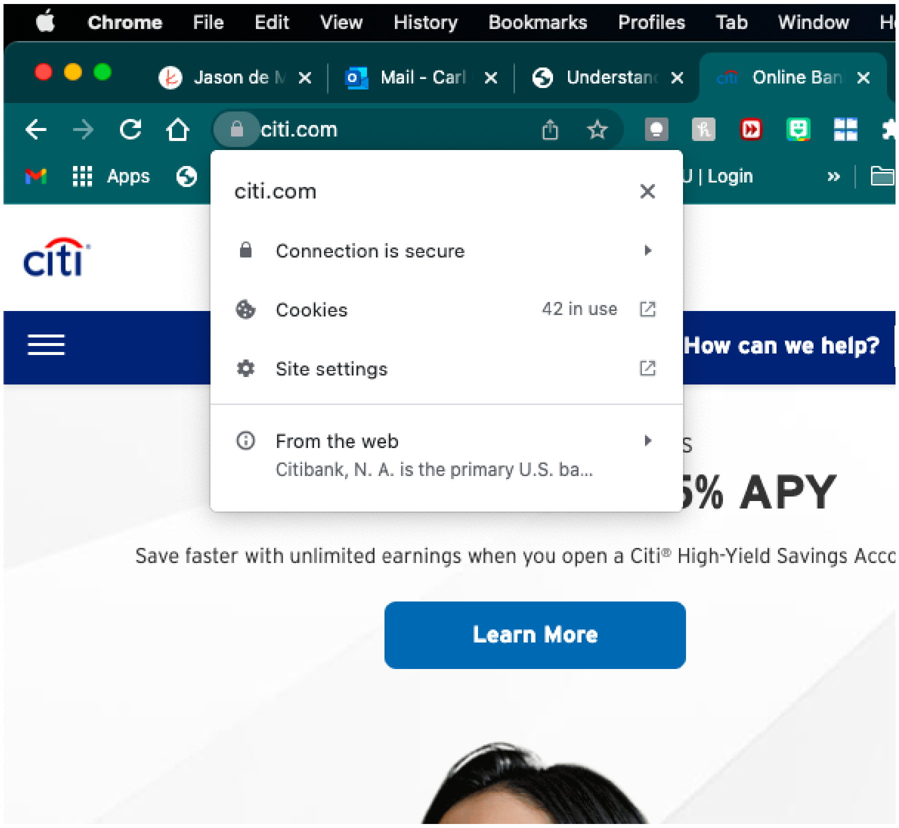
Since we have a short key of 128 bit, we will see some repetition of our key. By noticing patterns in the decrypted text being reused, we may be able to link back to what the original key is.

<u>2.4</u>

Given that we have a short message of 40 bit, the plaintext and key can potentially be a 40 bit as well. With brute force, we may get some type of success but won't know if our answer is truly the correct original plaintext. From the demonstration/proof in class on OTPs, it seems as if there is no clue or hint to harp on to ensure our success of hacking the message.

<u>P. 159-160 PDF</u>
Step 3 Parts A-B

I've gone to the website and clicked the lock all while on Google Chrome. I see that citibank.com reverts us to citi.com.



citi.com

Connection is secure

Cookies 42 in use

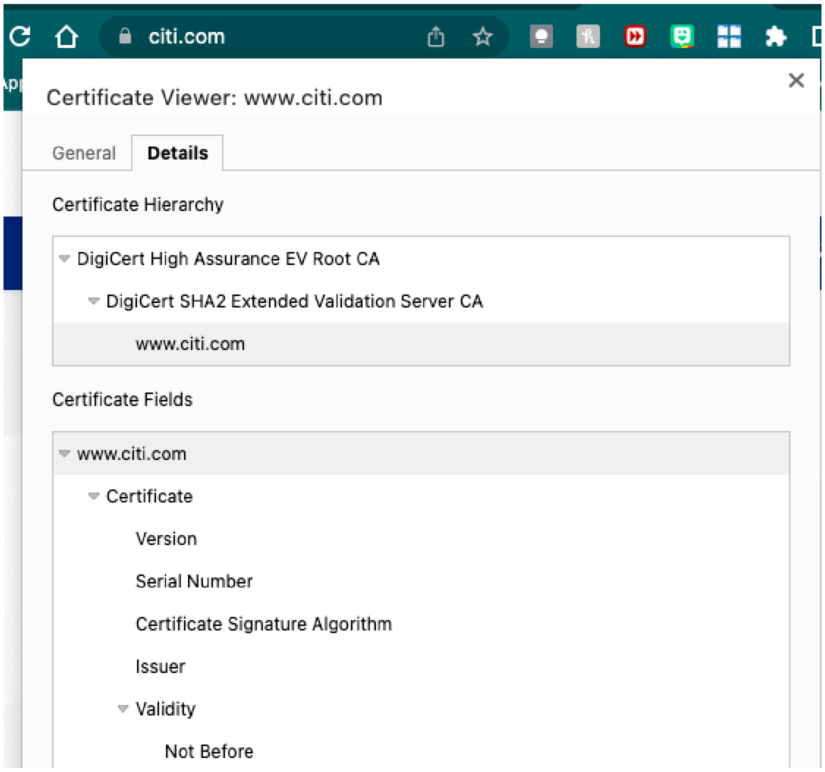
Site settings

From the web
Citibank, N. A. is the primary U.S. ba...

Save faster with unlimited earnings when you open a Citi® High-Yield Savings Acco

C

Taking a gander at the certificate information found under the details tab. This version of Chrome seems more updated than the textbook imagined. If this is not the correct details tab to show, please reach out and I can correct it.



Certificate Viewer: www.citi.com

General | **Details**

Certificate Hierarchy

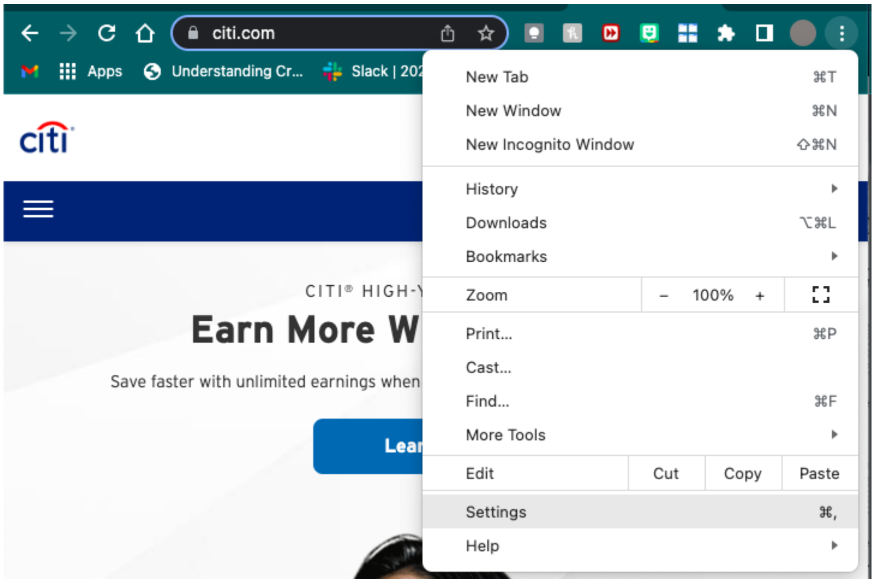
- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 Extended Validation Server CA
    - www.citi.com

Certificate Fields

- www.citi.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before

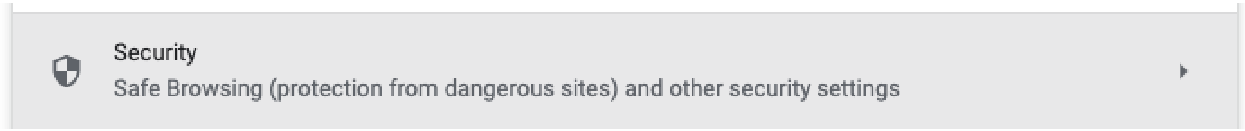
D,E, and F

I've gotten out of the certificate window, clicked the customize and control button, and am clicking settings.

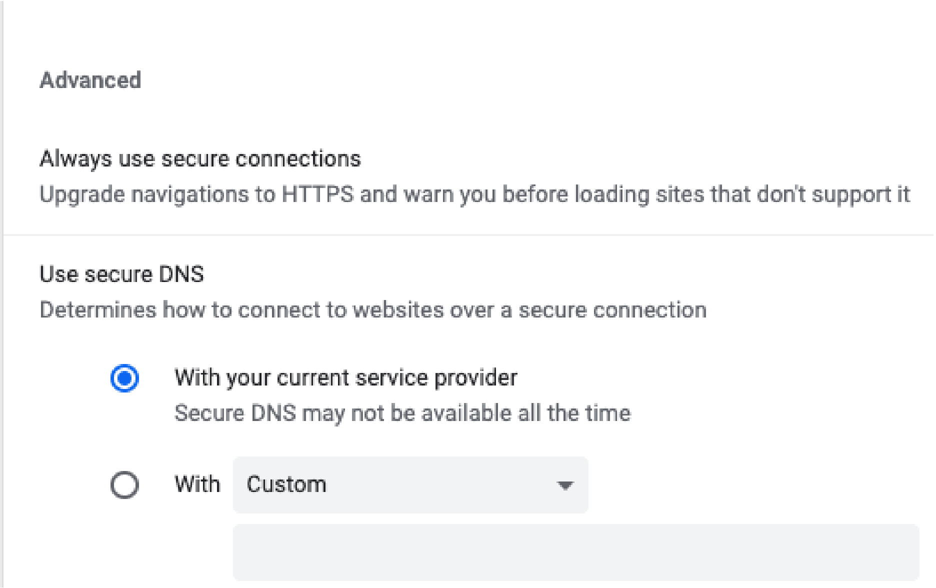


G

Finding security and heading to the Advanced section.



Security
Safe Browsing (protection from dangerous sites) and other security settings



Advanced

Always use secure connections
Upgrade navigations to HTTPS and warn you before loading sites that don't support it

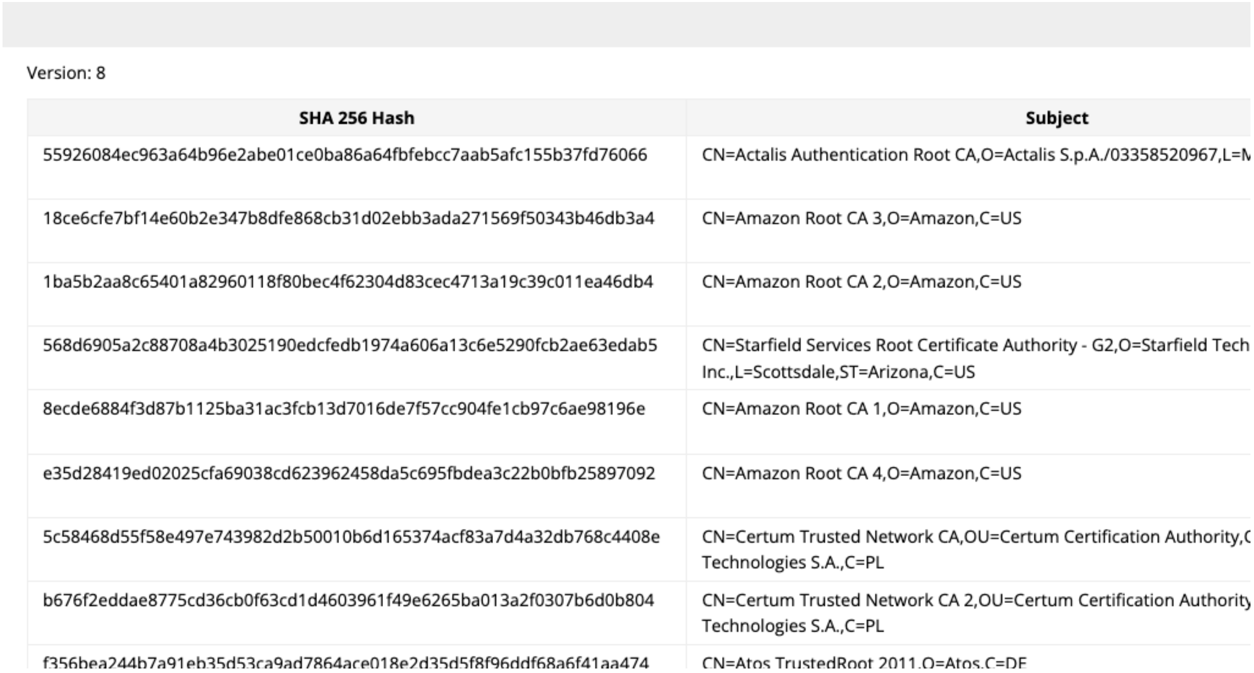
Use secure DNS
Determines how to connect to websites over a secure connection

● With your current service provider
Secure DNS may not be available all the time

○ With Custom

H

Scrolling down in Advanced and clicking Certificates managed by Chrome, I'm able to see Chrome's trusted root certificate store.



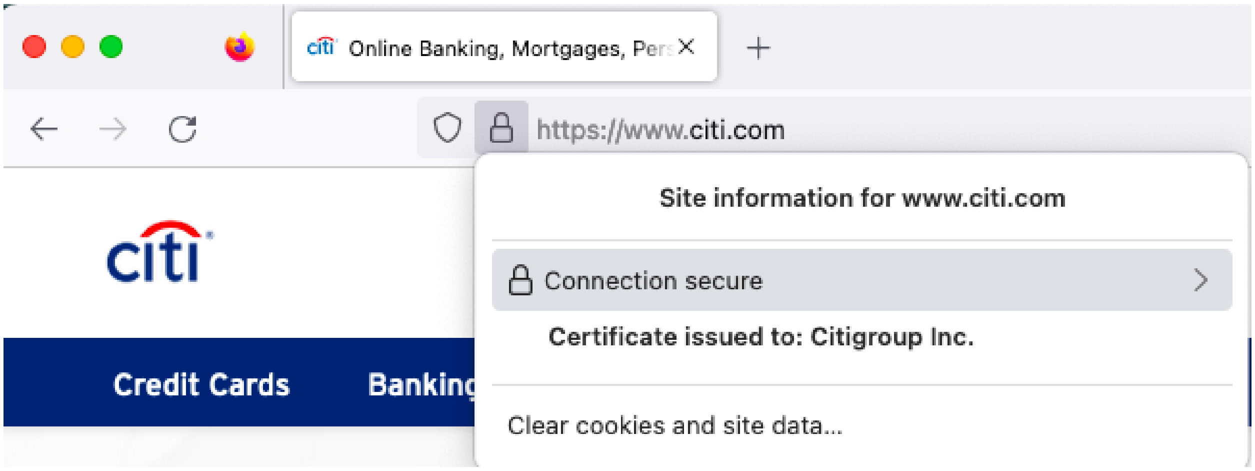
Version: 8

SHA 256 Hash	Subject
55926084ec963a64b96e2abe01ce0ba86a64fbfebcc7aab5afc155b37fd76066	CN=Actalis Authentication Root CA,O=Actalis S.p.A./03358520967,L=M
18ce6cfe7bf14e60b2e347b8dfe868cb31d02ebb3ada271569f50343b46db3a4	CN=Amazon Root CA 3,O=Amazon,C=US
1ba5b2aa8c65401a82960118f80bec4f62304d83cec4713a19c39c011ea46db4	CN=Amazon Root CA 2,O=Amazon,C=US
568d6905a2c88708a4b3025190edcfedb1974a606a13c6e5290fcb2ae63edab5	CN=Starfield Services Root Certificate Authority - G2,O=Starfield Tech Inc.,L=Scottsdale,ST=Arizona,C=US
8ecde6884f3d87b1125ba31ac3fcb13d7016de7f57cc904fe1cb97c6ae98196e	CN=Amazon Root CA 1,O=Amazon,C=US
e35d28419ed02025cfa69038cd623962458da5c695fbdea3c22b0bfb25897092	CN=Amazon Root CA 4,O=Amazon,C=US
5c58468d55f58e497e743982d2b50010b6d165374acf83a7d4a32db768c4408e	CN=Certum Trusted Network CA,OU=Certum Certification Authority,C Technologies S.A.,C=PL
b676f2eddae8775cd36cb0f63cd1d4603961f49e6265ba013a2f0307b6d0b804	CN=Certum Trusted Network CA 2,OU=Certum Certification Authority Technologies S.A.,C=PL
f356bea244b7a91eb35d53ca9ad7864ace018e2d35d5f8f96ddf68a6f41aa474	CN=Atos TrustedRoot 2011,O=Atos,C=DE

Step 4

Task A-B

Back at it again on citi.com via Mozilla and clicking the lock. Continuing to click Connection Secure.



Online Banking, Mortgages, Pers
https://www.citi.com
citi
Credit Cards
Banking

Site information for www.citi.com

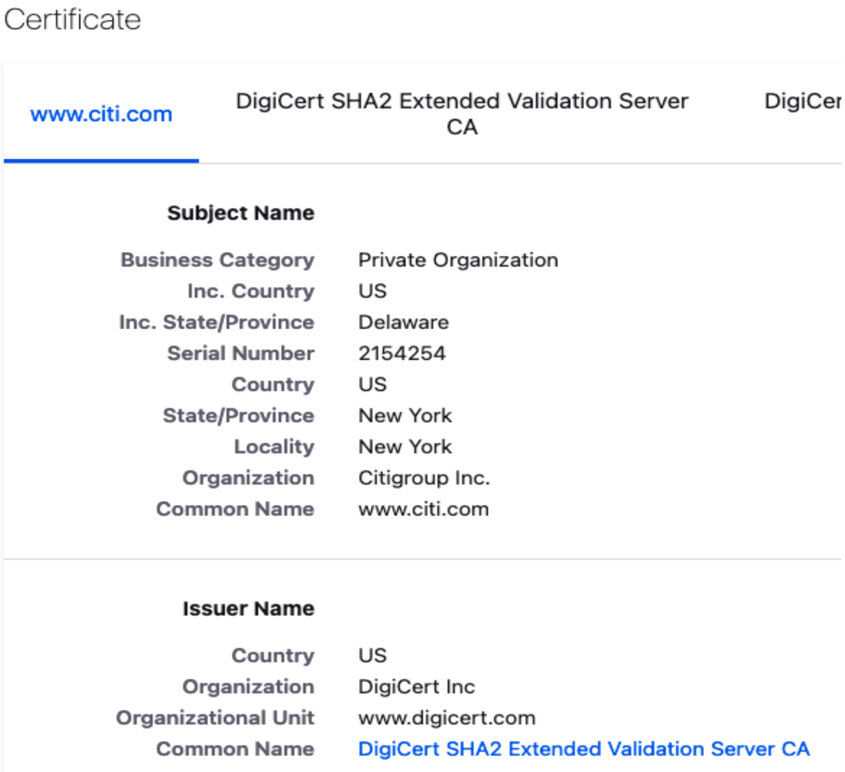
Connection secure

Certificate issued to: Citigroup Inc.

Clear cookies and site data...

Task C-F

Finding the information about the certificate, CA, and CA's root.



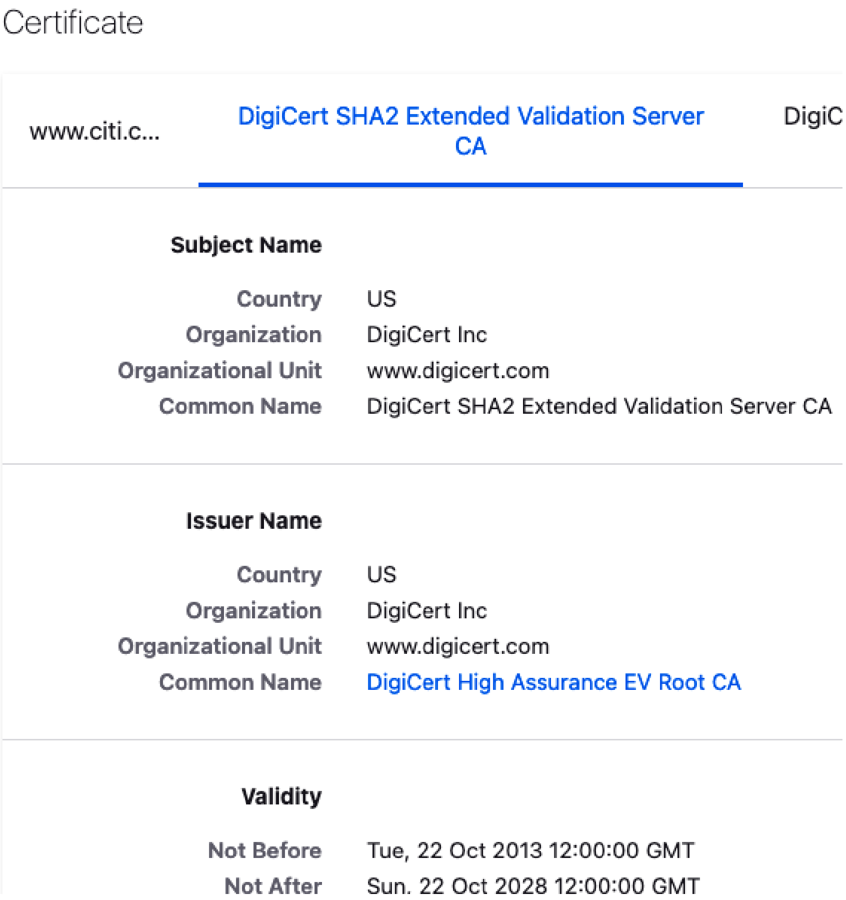
Certificate

Subject Name

Business Category	Private Organization
Inc. Country	US
Inc. State/Province	Delaware
Serial Number	2154254
Country	US
State/Province	New York
Locality	New York
Organization	Citigroup Inc.
Common Name	www.citi.com

Issuer Name

Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert SHA2 Extended Validation Server CA



Subject Name

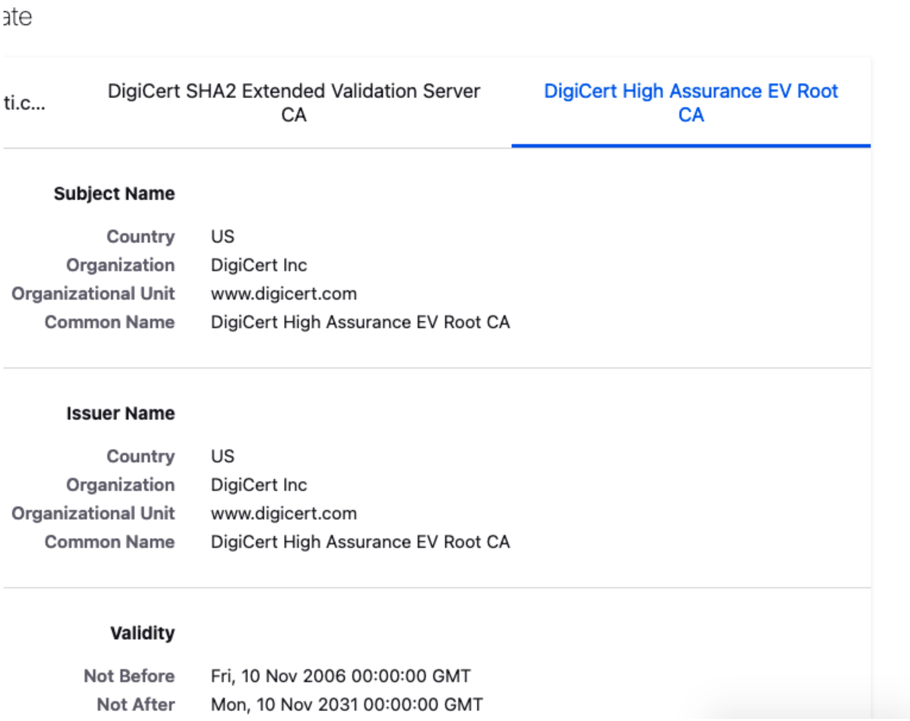
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert SHA2 Extended Validation Server CA

Issuer Name

Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert High Assurance EV Root CA

Validity

Not Before	Tue, 22 Oct 2013 12:00:00 GMT
Not After	Sun. 22 Oct 2028 12:00:00 GMT


ate
ti.c...
DigiCert SHA2 Extended Validation Server CA
DigiCert High Assurance EV Root CA

Subject Name

Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert High Assurance EV Root CA

Issuer Name

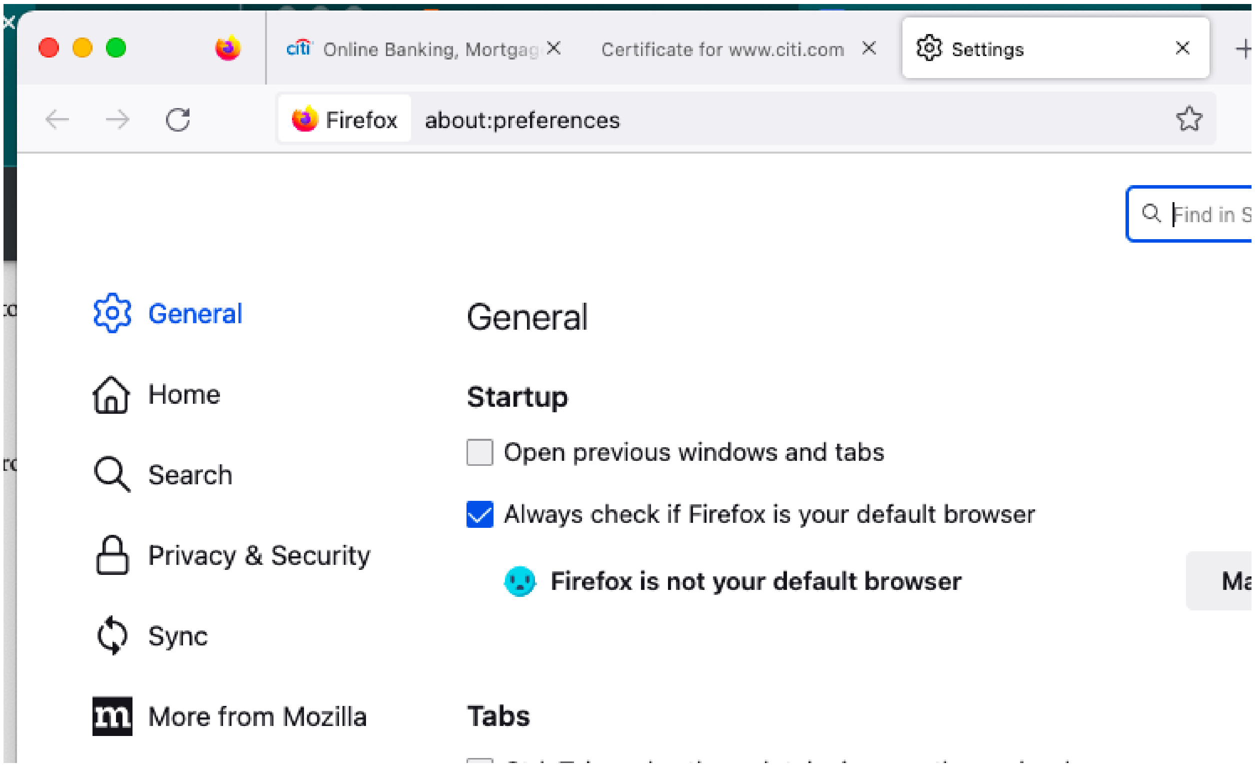
Country	US
Organization	DigiCert Inc
Organizational Unit	www.digicert.com
Common Name	DigiCert High Assurance EV Root CA

Validity

Not Before	Fri, 10 Nov 2006 00:00:00 GMT
Not After	Mon, 10 Nov 2031 00:00:00 GMT

Task G-H

Clicking the three horizontal lines, Preferences, and soon navigating to Privacy and Security.



about:preferences

General

Startup

□ Open previous windows and tabs

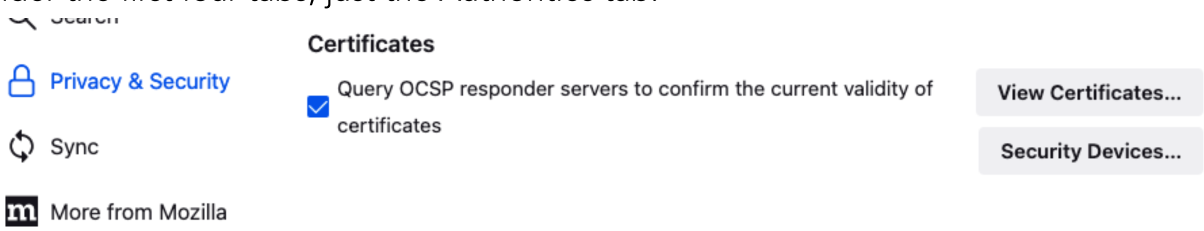
☑ Always check if Firefox is your default browser

Firefox is not your default browser

Tabs

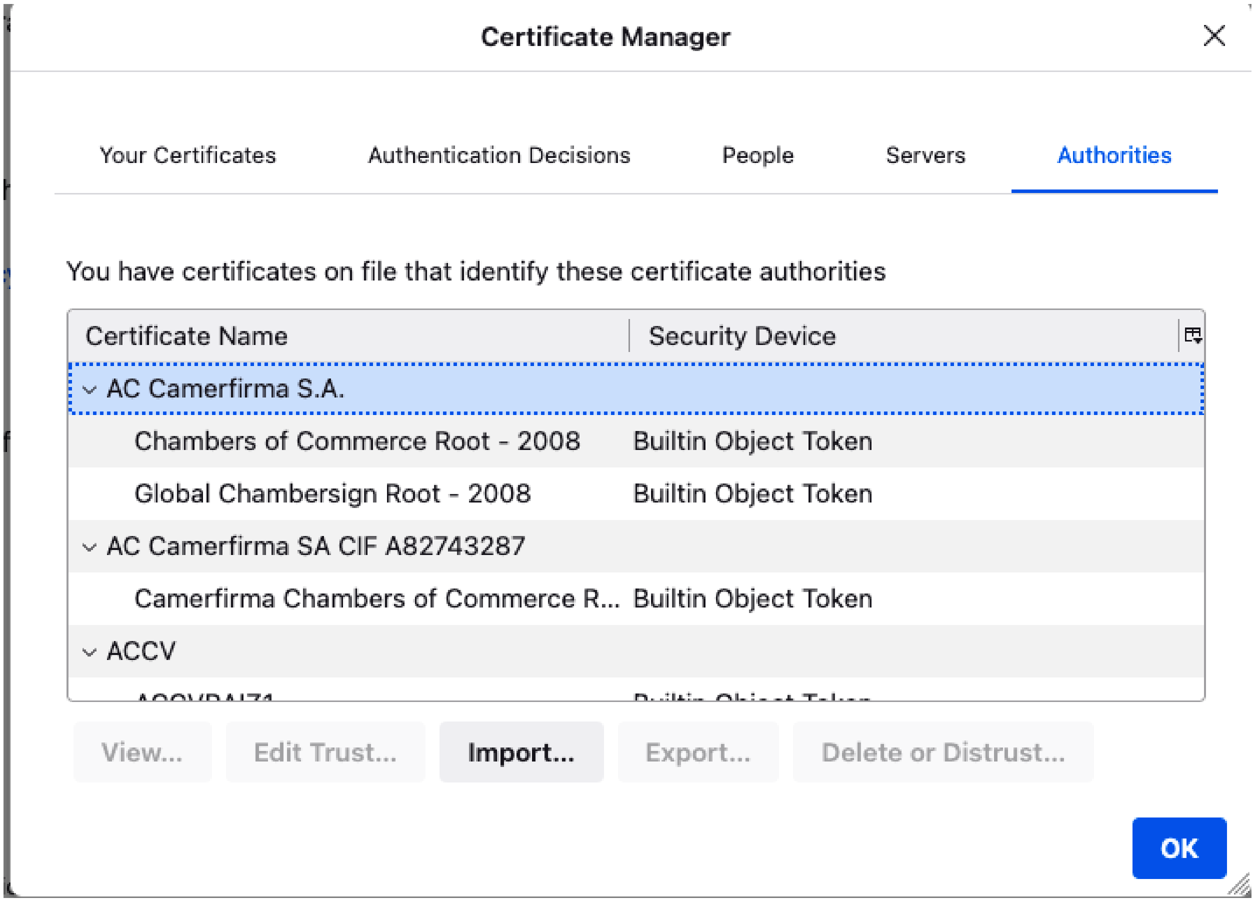
Task I-K

Clicked privacy and security, view certificates, and looked over Firefox's trusted root certificate store. Since I had to download Firefox for this task, I didn't have anything under the first four tabs; just the Authorities tab.



Certificates

☑ Query OCSP responder servers to confirm the current validity of certificates



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 R...	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token