Name: Hemant Jain

Lab Progress Report Due Date: 03/08/2021

Current Week Since Start Date: Week 7 (03/09/2021– 03/15/2021)

Reporting Week: From Mar 03, 2021 to Mar 08, 2021

Summary about the TestOut Module-7 Learning:

From the TestOut LabSim, I learnt about the Cryptography and PKI. Learnt about the three main concepts to understand when dealing with encryption methodology like Encryption, Hashing and Digital Signatures.

Asymmetric encryption methods, which use a public key to provide confidentiality and trust, are generally used to encrypt data transmitted over the internet. Proper management and safety of these keys is important. Public key infrastructure (PKI) provides an environment in which public encryption keys can be created and managed. At the heart of PKI are certificate authorities (CAs) who are responsible for issuing, validating, and revoking certificates.

Read about the CSR Information Common Name, SAN, Organization, Organizational Unit, City, State, Country, Email Address, Public Key. Learning about the Certificate Authority was a different along with the hands-on experience in creating and editing out the CA certificates and attributes. Encryption is the process of encoding data into something that is unreadable called ciphertext.

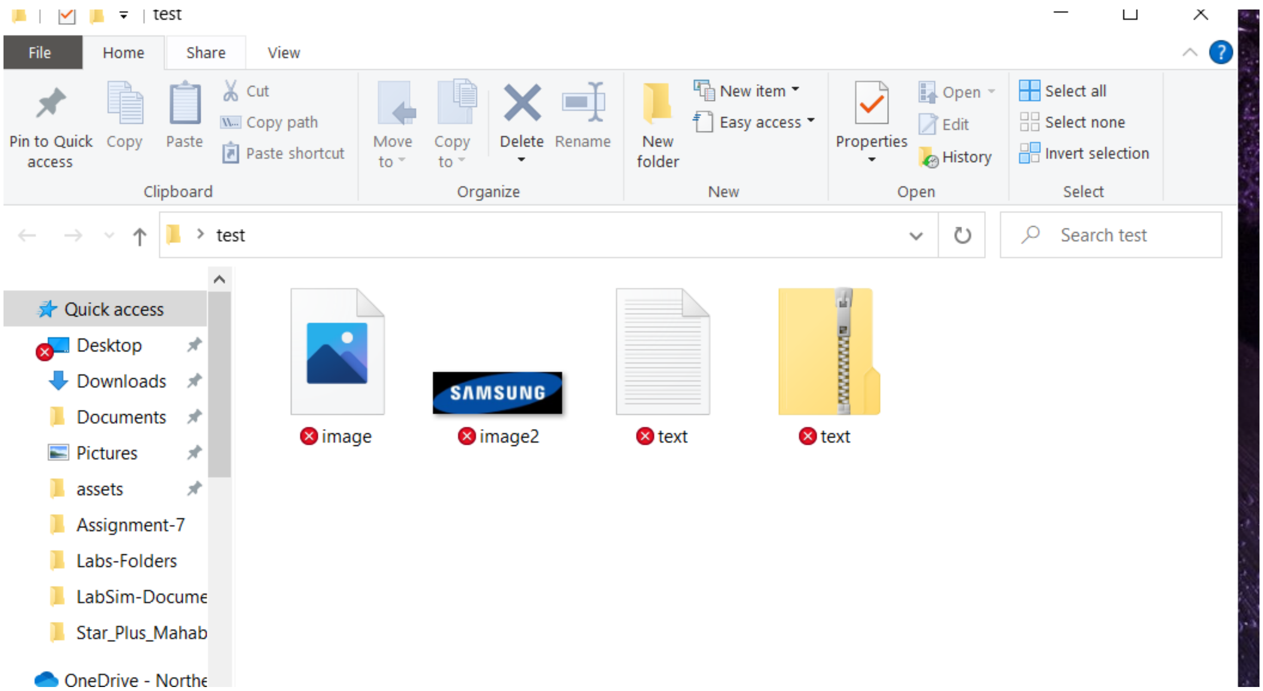
Reading about the different Symmetric Algorithms like Data Encryption Standard (DES), Rivest's Cipher(RC), Advanced Encryption Standard(AES), International Data Encryption Algorithm(IDEA),Blowfish, Twofish, CAST. And the asymmetric algorithms like Diffie-Hellman, Rivest-Shamir-Adleman(RSA), Digital Signature Algorithm, Elliptic Curve Cryptography(ECC). Hybrid cryptosystems combine the efficiency of symmetric encryption with the convenience of asymmetric encryption.
Hashing is the process of generating a fixed-length hexadecimal string value from any file type or data. Hashes can be generated from messages, image files, data files, and most other types of data. This output is known as the message digest or hash

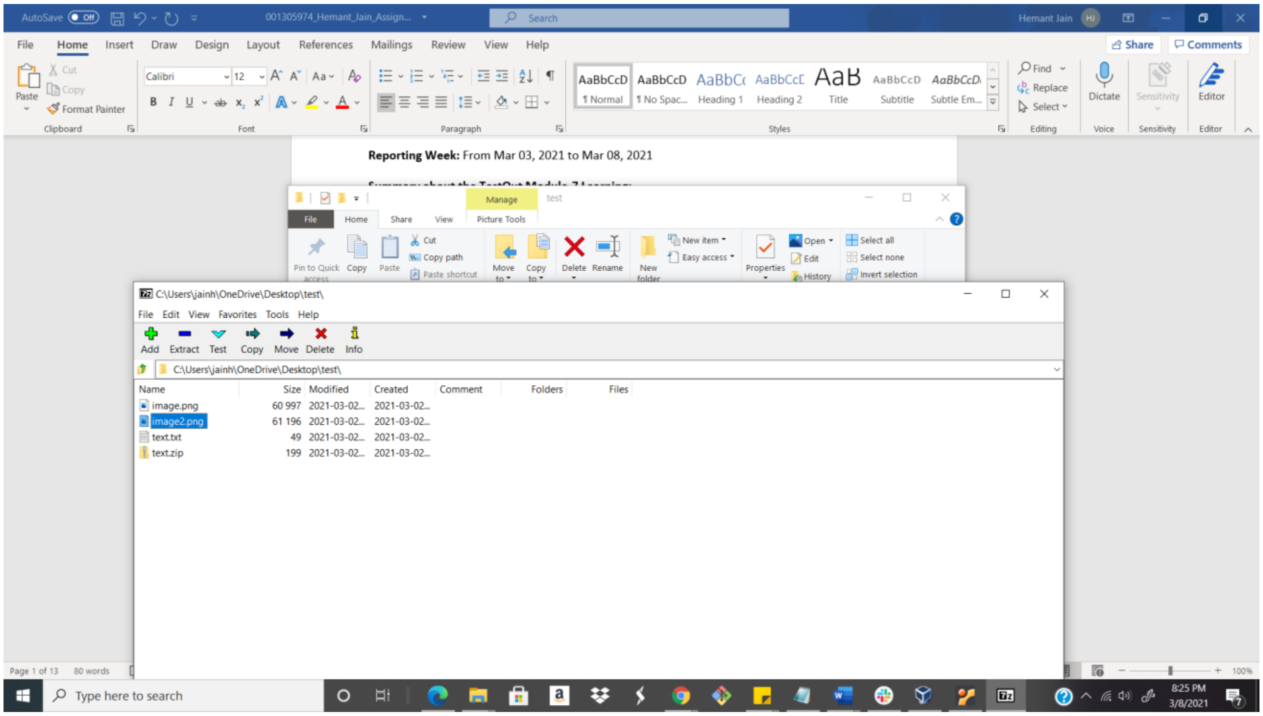
Ephemeral keys are keys that are generated for each new session or message sent. For example, perfect forward secrecy (PFC) uses ephemeral keys.

EFS provides an easy and seamless way for users to encrypt files on their Windows computers. EFS is only used to encrypt individual files and folders. he encryption and decryption process rely on the user's password being kept safe. If the user account becomes corrupted or the password is forgotten, any encrypted files are lost. To help remedy this, a data recovery agent(DRA) can be setup-ed.

In-class Lab Homework:

Class Lab Screenshots:

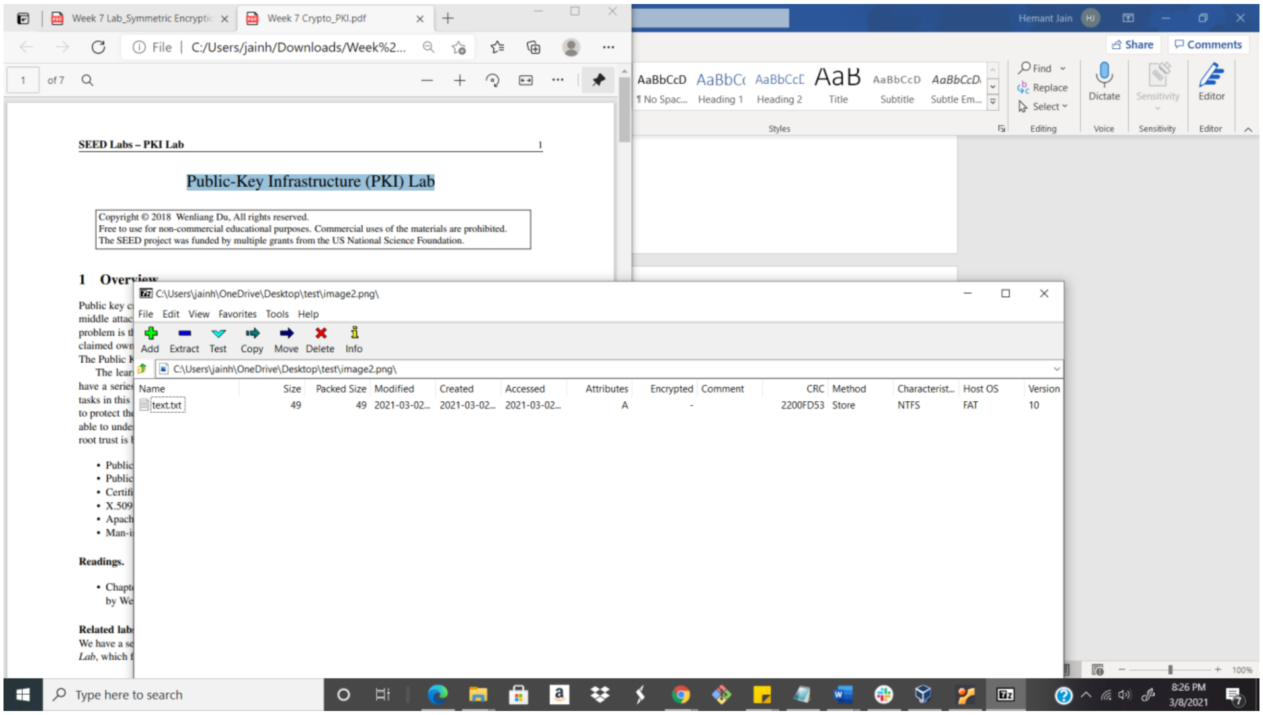




Reporting Week: From Mar 03, 2021 to Mar 08, 2021

C:\Users\jainh\OneDrive\Desktop\test\

Name	Size	Modified	Created	Comment	Folders	Files
image.png	60 997	2021-03-02...	2021-03-02...			
image2.png	61 196	2021-03-02...	2021-03-02...			
text.txt	49	2021-03-02...	2021-03-02...			
text.zip	199	2021-03-02...	2021-03-02...			



SEED Labs – PKI Lab

Public-Key Infrastructure (PKI) Lab

Copyright © 2018 Wenliang Du, All rights reserved.
Free to use for non-commercial educational purposes. Commercial uses of the materials are prohibited.
The SEED project was funded by multiple grants from the US National Science Foundation.

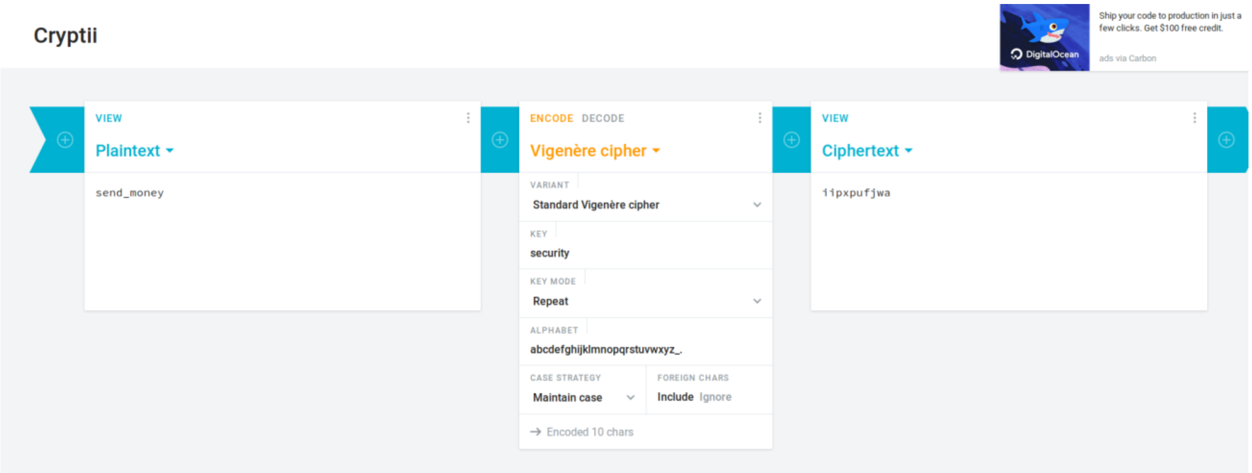
C:\Users\jainh\OneDrive\Desktop\test\image2.png\

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment	CRC	Method	Characterist...	Host OS	Version
text.txt	49	49	2021-03-02...	2021-03-02...	2021-03-02...	A	-		2200FD53	Store	NTFS	FAT	10

Part-1 Assignment Lab:

Question-1: What is the ciphertext when encrypting "send_money" with the key "security" and alphabet abcdefghijklmnopqrstuvwxyz_.?

Ans: iipxpufjwa



send_money

VARIANT: Standard Vigenère cipher

KEY: security

KEY MODE: Repeat

ALPHABET: abcdefghijklmnopqrstuvwxyz_.

CASE STRATEGY: Maintain case

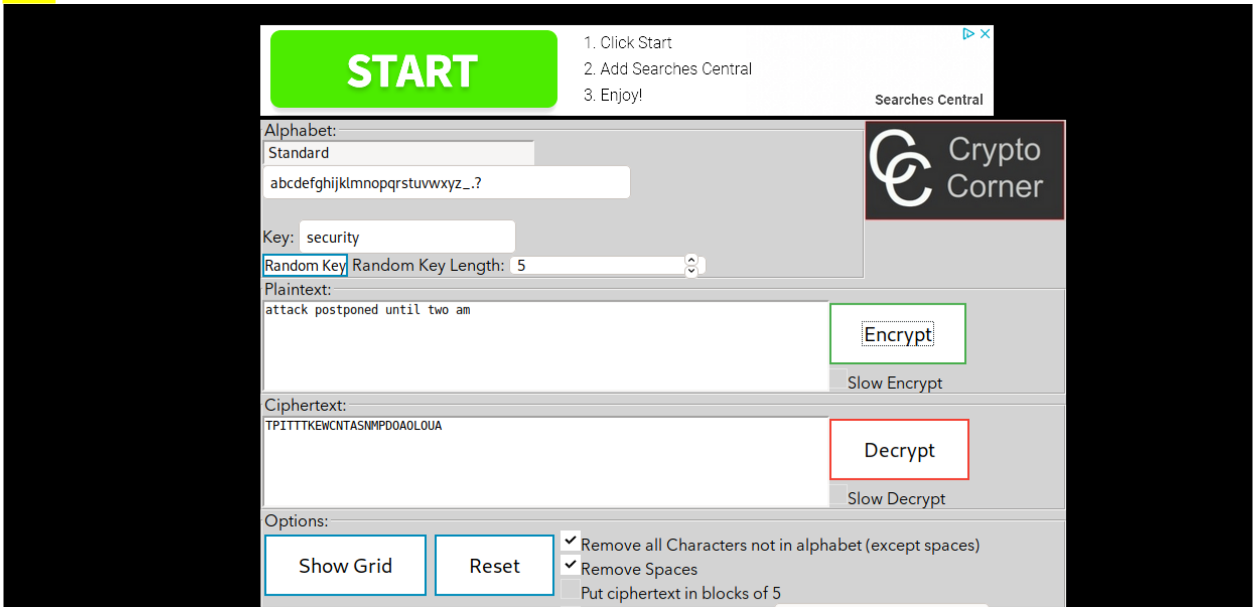
FOREIGN CHARS: Include Ignore

→ Encoded 10 chars

iipxpufjwa

Question-2: What is the ciphertext when encrypting "attack postponed until two am" with the provided key

Ans: **TPITTTKEWCNTASNMPDOAOLOUA**



Alphabet: Standard

abcdefghijklmnopqrstuvwxyz_.?

Key: security

Random Key Length: 5

Plaintext:

```
attack postponed until two am
```

Ciphertext:

```
TPITTTKEWCNTASNMPDOAOLOUA
```

Options:

☑ Remove all Characters not in alphabet (except spaces)

☑ Remove Spaces

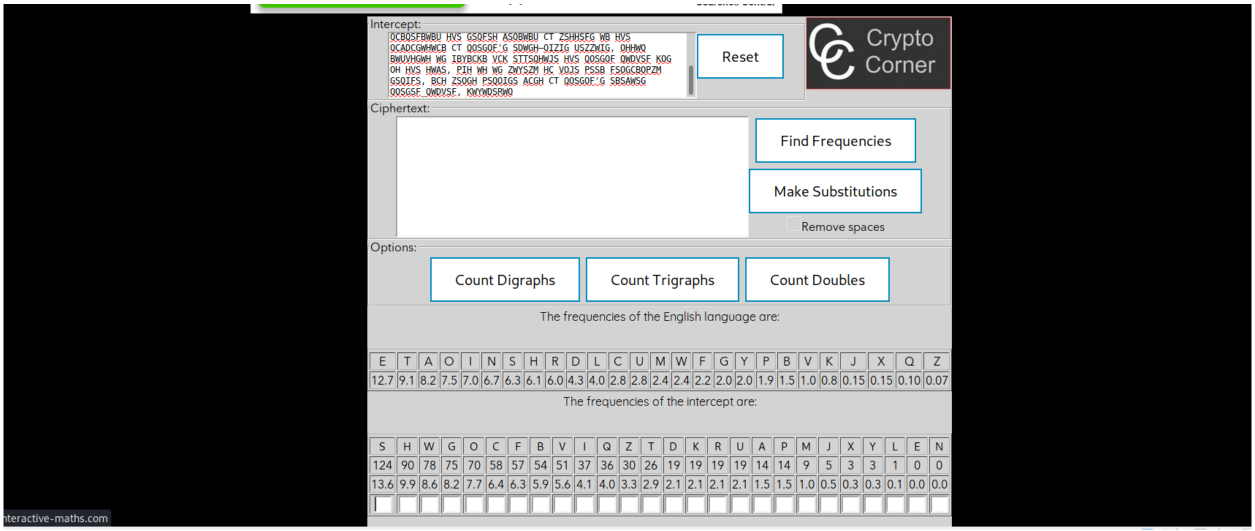
□ Put ciphertext in blocks of 5

Frequency Analysis

Questions: 1. What are the four most frequent characters, in descending order? Examine the frequency table chart at h ttp://en.wikipedia.org/wiki/Frequency_analysis. What does this suggest the four letters identified correspond to?

Question: What are the four most frequent characters?

Ans: S,H,W,G



Intercept:

```
QCBQSFBWBU HVS GSQFSH ASQBWBU CT ZSHHSFG WB HVS
QCADCGWHWCB CT QOSGOF'G SDWGH—OIZIG USZZWIG, OHHWQ
BWUVHGWH WG IBYBCKB VCK STTSQHWJS HVS QOSGOF QWDVSF KOG
OH HVS HWAS, PIH WH WG ZWYSZM HC VOJS PSSB FSOGCBOPZM
GSQIFS, BCH ZSOGH PSQOIGS ACGH CT QOSGOF'G SBSAWSG
QOSGSF QWDVSF, KWYWDSRWO
```

Ciphertext:

Options:

The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

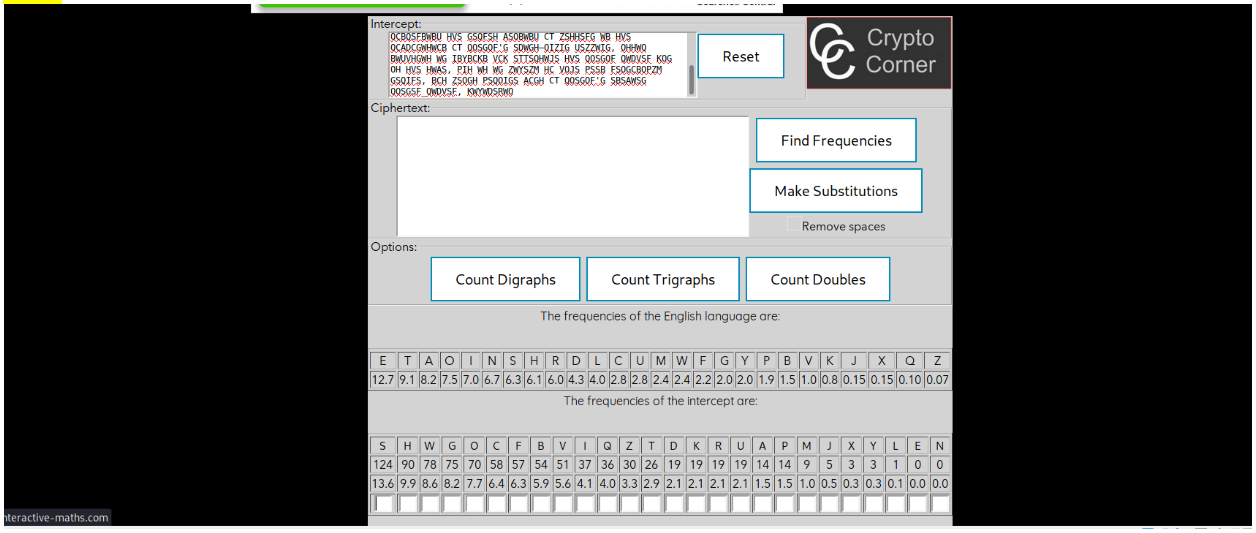
The frequencies of the intercept are:

S	H	W	G	O	C	F	B	V	I	Q	Z	T	D	K	R	U	A	P	M	J	X	Y	L	E	N
124	90	78	75	70	58	57	54	51	37	36	30	26	19	19	19	19	14	14	9	5	3	3	1	0	0
13.6	9.9	8.6	8.2	7.7	6.4	6.3	5.9	5.6	4.1	4.0	3.3	2.9	2.1	2.1	2.1	2.1	1.5	1.5	1.0	0.5	0.3	0.3	0.1	0.0	0.0

2. Analyze bigrams and trigrams in the ciphertext. What do the most frequent ciphertext bigrams suggest the three 2-length N-grams identified correspond to in English plaintext? Also examine N-grams of length 3 and report the likely plaintext identities of the four 3-length N-grams reported. (Use h ttp://en.wikipedia.org/wiki/Trigram).

Question: What are the three most frequent trigrams?

Ans:



Intercept:

```
QCBQSFBWBU HVS GSQFSH ASQBWBU CT ZSHHSFG WB HVS
QCADCGWHWCB CT QOSGOF'G SDWGH—OIZIG USZZWIG, OHHWQ
BWUVHGWH WG IBYBCKB VCK STTSQHWJS HVS QOSGOF QWDVSF KOG
OH HVS HWAS, PIH WH WG ZWYSZM HC VOJS PSSB FSOGCBOPZM
GSQIFS, BCH ZSOGH PSQOIGS ACGH CT QOSGOF'G SBSAWSG
QOSGSF QWDVSF, KWYWDSRWO
```

Ciphertext:

Options:

The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

The frequencies of the intercept are:

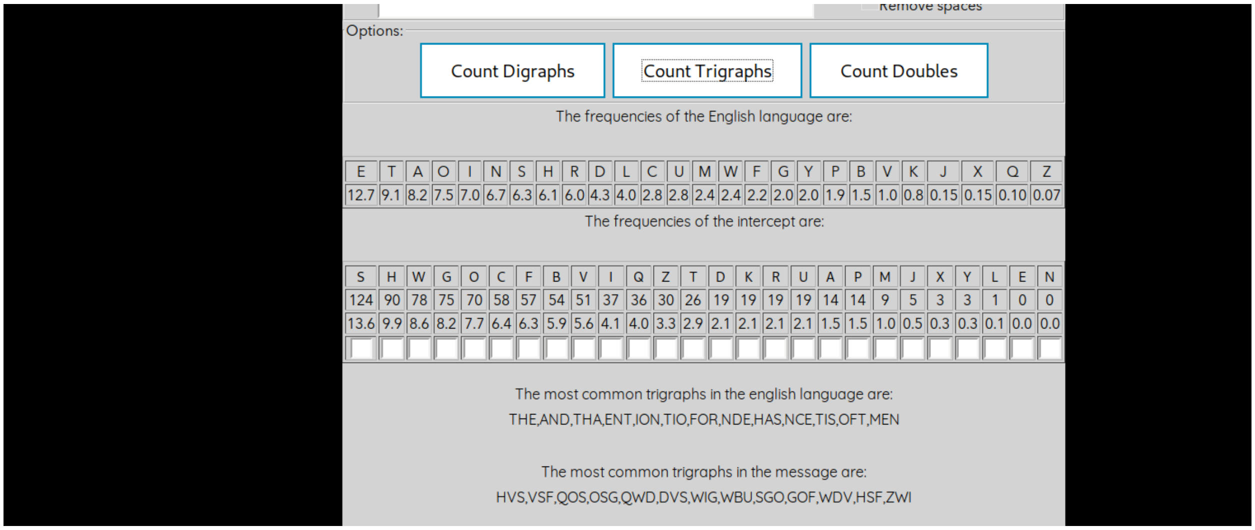
S	H	W	G	O	C	F	B	V	I	Q	Z	T	D	K	R	U	A	P	M	J	X	Y	L	E	N
124	90	78	75	70	58	57	54	51	37	36	30	26	19	19	19	19	14	14	9	5	3	3	1	0	0
13.6	9.9	8.6	8.2	7.7	6.4	6.3	5.9	5.6	4.1	4.0	3.3	2.9	2.1	2.1	2.1	2.1	1.5	1.5	1.0	0.5	0.3	0.3	0.1	0.0	0.0

The most common trigraphs in the english language are:

THE, AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are:

HVS,VSF,QOS,OSG,QWD,DVS,WIG,WBU,SGO,GOF,WDV,HSF,ZWI



The frequencies of the English language are:

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	X	Q	Z
12.7	9.1	8.2	7.5	7.0	6.7	6.3	6.1	6.0	4.3	4.0	2.8	2.8	2.4	2.4	2.2	2.0	2.0	1.9	1.5	1.0	0.8	0.15	0.15	0.10	0.07

The frequencies of the intercept are:

S	H	W	G	O	C	F	B	V	I	Q	Z	T	D	K	R	U	A	P	M	J	X	Y	L	E	N
124	90	78	75	70	58	57	54	51	37	36	30	26	19	19	19	19	14	14	9	5	3	3	1	0	0
13.6	9.9	8.6	8.2	7.7	6.4	6.3	5.9	5.6	4.1	4.0	3.3	2.9	2.1	2.1	2.1	2.1	1.5	1.5	1.0	0.5	0.3	0.3	0.1	0.0	0.0

The most common trigraphs in the english language are:
THE,AND,THA,ENT,ION,TIO,FOR,NDE,HAS,NCE,TIS,OFT,MEN

The most common trigraphs in the message are:
HVS,VSF,QOS,OSG,QWD,DVS,WIG,WBU,SGO,GOF,WDV,HSF,ZWI

3. Assume that a simple cipher that shifts all characters by a fixed number was used to create the cipertext. Given the results of the frequency analysis, what would the shift key have been (the shift to go from plaintext to ciphertext)? Don't be proud; you can use your fingers to count.

Question: What is the key of the ciphertext, counting forwards?

Ans: The key is 14

4. What is the plaintext? Question: What author is quoted in the plaintext? **SUETONIUS**

Ans: THE CAESAR CIPHER IS NAMED AFTER JULIUS CAESAR, WHO, ACCORDING TO SUETONIUS, USED IT WITH A SHIFT OF THREE TO PROTECT

MESSAGES OF MILITARY SIGNIFICANCE. W IF HE HAD ANYTHING CONFIDENTIAL TO SAY, HE WROTE IT IN CIPHER, THAT IS, BY SO CHANGING THE ORDER OF THE LETTERS OF THE ALPHABET, THAT NOT A WORD COULD BE—SUETONIUS, LIFE OF JULIUS CAESAR 56HIS NEPHEW, AUGUSTUS, ALSO USED THE CIPHER, BUT WITH A RIGHT SHIFT OF ONE, AND IT DID NOT WRAP AROUND TO THE BEGINNING OF THE ALPHABET: WHENEVER HE WROTE IN CIPHER, HE WROTE B FOR A, C FOR B, AND THE REST OF THE LETTERS ON THE SAME PRINCIPLE, USING AA FOR X.—SUETONIUS, LIFE OF AUGUSTUS 88THERE IS EVIDENCE THAT JULIUS CAESAR USED MORE COMPLICATED SYSTEMS AS WELL, AND ONE WRITER, AULUS GELLIUS, REFERS TO A (NOW LOST) TREATISE ON HIS CIPHERS: THERE IS EVEN A RATHER INGENIOUSLY WRITTEN TREATISE BY THE GRAMMARIAN PROBUS CONCERNING THE SECRET MEANING OF LETTERS IN THE COMPOSITION OF CAESAR'S EPIST—AULUS GELLIUS, ATTIC NIGHTSIT IS UNKNOWN HOW EFFECTIVE THE CAESAR CIPHER WAS AT THE TIME, BUT IT IS LIKELY TO HAVE BEEN REASONABLY SECURE, NOT LEAST BECAUSE MOST OF CAESAR'S ENEMIES CAESER_CIPHER, WIKIPEDIA

Ciphertext (hexadecimal): E0 C5 B5 B0 82 9A 8A DA B8 FD 8A 9E 67 5A 57

1. One-time pad 1: A1 B1 C1 D1 E1 F1 AA BB CC DD EE FF 10 34 76

Question: What is the plaintext using the one-time pad 1?

Ans: Attack at dawn!

2. One-time pad 2: B2 A0 C1 C2 E7 FB FE FA D9 89 AA AF 56 6A 67

Question: What is the plaintext using the one-time pad 2?

Ans: Retreat at 1100

3. One-time pad 3: B3 B0 C7 C2 E7 F4 EE BF CA DD EC F1 15 2E 76

Question: What is the plaintext using the one-time pad 3?

Ans: Surrender fort!

4. One-time pad 4: B4 AD D0 90 E1 FB FE FA D1 8E AA FA 02 3B 33

Question: What is the plaintext using the one-time pad 4?

Ans: The cat is dead

Question: How many possible plaintexts exist for this one-time-pad ciphertext?

Ans: Infinite

Part-2 Hashing

Questions:

1. What is the length of each of the following algorithm hashes in bytes? MD5, SHA-1, SHA-256, SHA-512? How many bits does each hash represent?

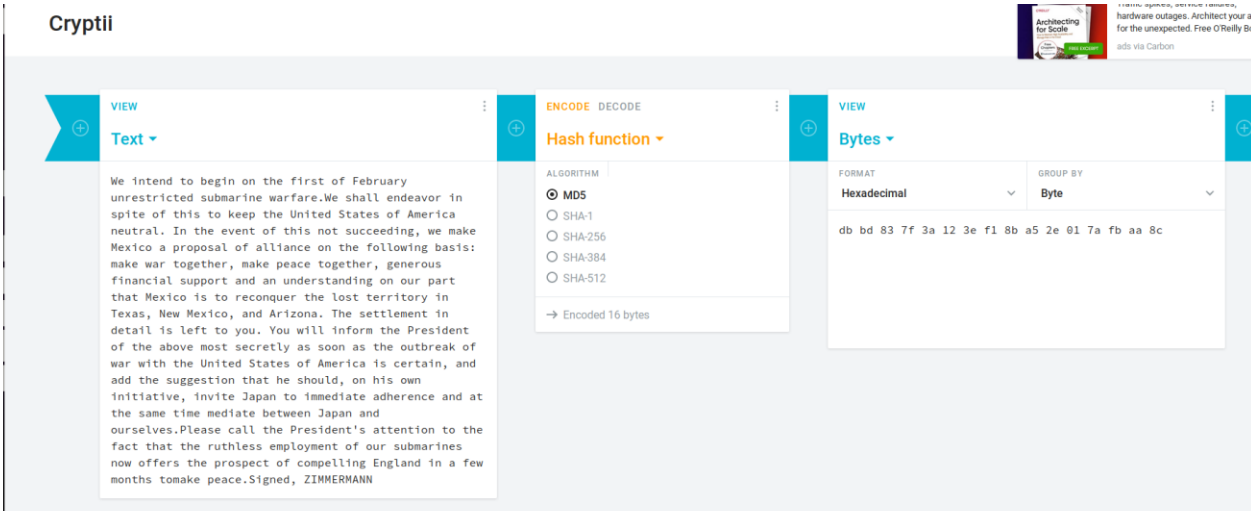
Ans: MD5 : 16 bytes(128 bits) , SHA-1 : 20 bytes(160 bits) , SHA-256: 32 bytes(256bits) , SHA-512: 64 bytes(512bits)

(hint: how many bits are in one hex digit – also called a 'nibble'? How many nibbles in the key? Or, How many bits in a byte, and how many bytes in a two-digit hex number like 'FA'? Review this if you're still stuck)

Question: How many bits are in an MD5 hash?

Ans: 128 bits

Ans: db bd 83 7f 3a 12 3e f1 8b a5 2e 01 7a fb aa 8c (Bytes)



```
We intend to begin on the first of February
unrestricted submarine warfare.We shall endeavor in
spite of this to keep the United States of America
neutral. In the event of this not succeeding, we make
Mexico a proposal of alliance on the following basis:
make war together, make peace together, generous
financial support and an understanding on our part
that Mexico is to reconquer the lost territory in
Texas, New Mexico, and Arizona. The settlement in
detail is left to you. You will inform the President
of the above most secretly as soon as the outbreak of
war with the United States of America is certain, and
add the suggestion that he should, on his own
initiative, invite Japan to immediate adherence and at
the same time mediate between Japan and
ourselves.Please call the President's attention to the
fact that the ruthless employment of our submarines
now offers the prospect of compelling England in a few
months tomake peace.Signed, ZIMMERMANN
```

ALGORITHM
● MD5
○ SHA-1
○ SHA-256
○ SHA-384
○ SHA-512

→ Encoded 16 bytes

FORMAT: Hexadecimal
GROUP BY: Byte

```
db bd 83 7f 3a 12 3e f1 8b a5 2e 01 7a fb aa 8c
```

➔ 16*8 = 128 bits

Change just a single bit in content that you are hashing. e.g, change an “A” — 1010 to a B — 1011. Examine the hashes of the modified content. Since you only changed a single bit in a file of billions of bits, you might reason that the hashes would be nearly the same. Are they?

In cryptii, you can switch to a hex view thusly in order to make your single-bit-edit easier:

Question: Assume a 10 GB file is hashed. If only one bit is changed on a 10 GB file and then it is hashed again, how will the second hash compare to the first?

Ans: Completely different new hash value will be generated if only one single bit is changed in the 10GB file.

Question: Which property of cryptographic hash functions is most related to the previous question?

Ans: In cryptography, the avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The actual term was first used by Horst Feistel, although the concept dates back to at least Shannon's diffusion.

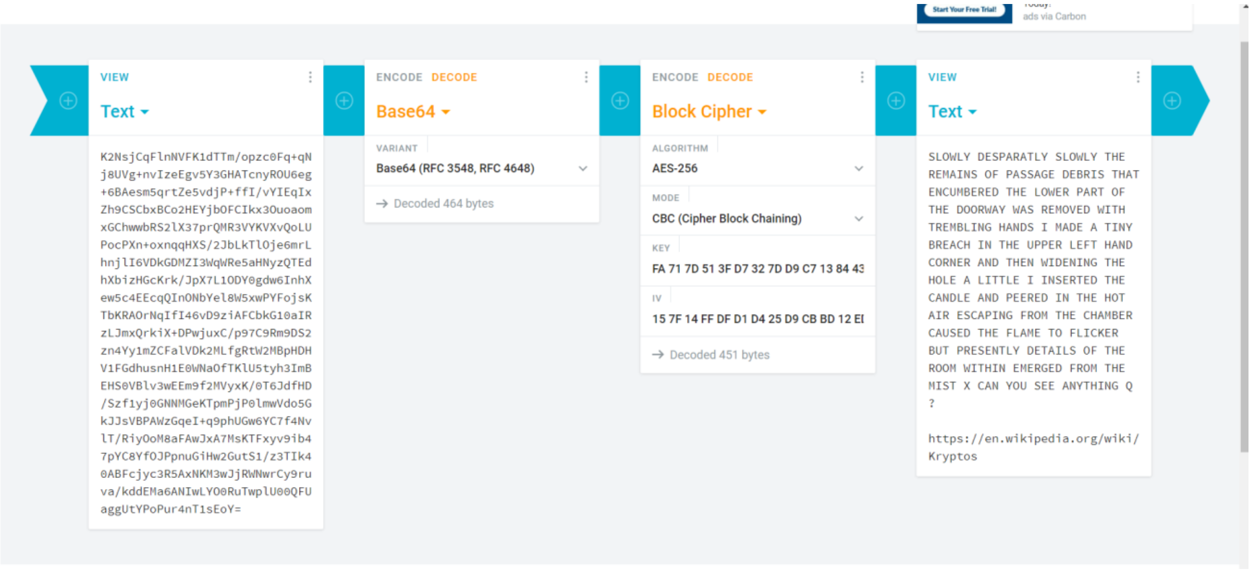
The SHA-1 hash function exhibits good avalanche effect. When a single bit is changed the hash sum becomes completely different.

If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a cryptanalyst can make predictions about the input, being given only the output. This may be sufficient to partially or completely break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device.

Constructing a cipher or hash to exhibit a substantial avalanche effect is one of the primary design objectives, and mathematically the construction takes advantage of the butterfly effect. This is why most block ciphers are product ciphers. It is also why hash functions have large data blocks. Both of these features allow small changes to propagate rapidly through iterations of the algorithm, such that every bit of the output should depend on every bit of the input before the algorithm terminates.

Symmetric Encryption with AES

What is the plaintext of the message?



```
K2NsjCqFlnNVFK1dTTm/opzc0Fq+qN
j8UVg+nvIzeEgv5Y3GHATcnyROU6eg
+6BAesm5qrtZe5vdjP+ffI/vYIEqIx
Zh9CSCbxBCo2HEYjbOFCIkx3Ouoaom
xGChwwbRS2lX37prQMR3VYKVXvQoLU
PocPXn+oxnqqHXS/2JbLkTlOje6mrL
hnjlI6VDkGDMZI3WqWRe5aHNyzQTEd
hXbizHGcKrk/JpX7L1ODY0gdw6InhX
ew5c4EEcqQInONbYel8W5xwPYFojsK
TbKRAOrNqIfI46vD9ziAFCbkG10aIR
zLJmxQrkiX+DPwjuxC/p97C9Rm9DS2
zn4Yy1mZCFalVDk2MLfgRtW2MBpHDH
V1FGdhusnH1E0WNaOfTKlU5tyh3ImB
EHS0VBlv3wEEm9f2MVyxK/0T6JdfHD
/Szf1yj0GNNMGeKTpmPjP0lmwVdo5G
kJJsVBPAWzGqeI+q9phUGw6YC7f4Nv
lT/RiyOoM8aFAwJxA7MsKTFxyv9ib4
7pYC8YfOJPpnuGiHw2GutS1/z3TIk4
0ABFcjyc3R5AxNKM3wJjRWNwrCy9ru
va/kddEMa6ANIwLYO0RuTwplU00QFU
aggUtYPoPur4nT1sEoY=
```

VARIANT
Base64 (RFC 3548, RFC 4648)

ALGORITHM
AES-256

MODE
CBC (Cipher Block Chaining)

KEY
FA 71 7D 51 3F D7 32 7D D9 C7 13 84 43

IV
15 7F 14 FF DF D1 D4 25 D9 CB BD 12 E

```
SLOWLY DESPARATLY SLOWLY THE
REMAINS OF PASSAGE DEBRIS THAT
ENCUMBERED THE LOWER PART OF
THE DOORWAY WAS REMOVED WITH
TREMBLING HANDS I MADE A TINY
BREACH IN THE UPPER LEFT HAND
CORNER AND THEN WIDENING THE
HOLE A LITTLE I INSERTED THE
CANDLE AND PEERED IN THE HOT
AIR ESCAPING FROM THE CHAMBER
CAUSED THE FLAME TO FLICKER
BUT PRESENTLY DETAILS OF THE
ROOM WITHIN EMERGED FROM THE
MIST X CAN YOU SEE ANYTHING Q
?

https://en.wikipedia.org/wiki/
Kryptos
```

Question: What is the URL included in the plaintext you decrypted with AES?

Ans: https://en.wikipedia.org/wiki/Kryptos

Message Sharing

key=19513FDC9DA4FB72A4A05EB66917548D3C90FF94D5419E1F2363EEA89DFEE1DD

iv =A74AA670A5B4FFB3898B272BCFEC7FC3

1. Question: How did you ensure that the key exchange was safe? How would you exchange keys if you were not in the same location?

Ans: Key exchange (also key establishment) is a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If it is an asymmetric key cipher with the public/private key property, both will need the other's public key.

There are two main ways**: Key Encapsulation Mechanism (KEM), or a Key Exchange (KEX).**

In a KEM, Alice will create a symmetric key from a CSPRNG or TRNG, sign it with a private key and encrypt it with Bob's public key. RSA would be a scheme that can handle this.

The other option is KEX. This is when Alice and Bob both generate ephemeral keys (with ECC for example). They both sign their ephemeral public keys with their static private keys and send them to each other. Both Alice and Bob combine their own ephemeral private key with the other's ephemeral public key (EC point multiplication in the case of ECC), and end up with the same shared secret. This is a point on the elliptic curve, so it will be passed through HKDF, into the correct format and length for the symmetric key.

This symmetric key MUST NOT be public, as it would defeat the point of encryption as anyone could decrypt the ciphertext.

2. Question: Which of the parameters of a block cipher (e.g., algorithm name, mode of operation, IV (if any), key length) are essential to keep secret? Security through obscurity does not count as "essential".

Ans:

I believe that it is essential that you keep the key secret.

If there is any other aspect of the cipher that you must keep secret (that is, you become insecure if it is revealed), then your cipher is 'broken'.

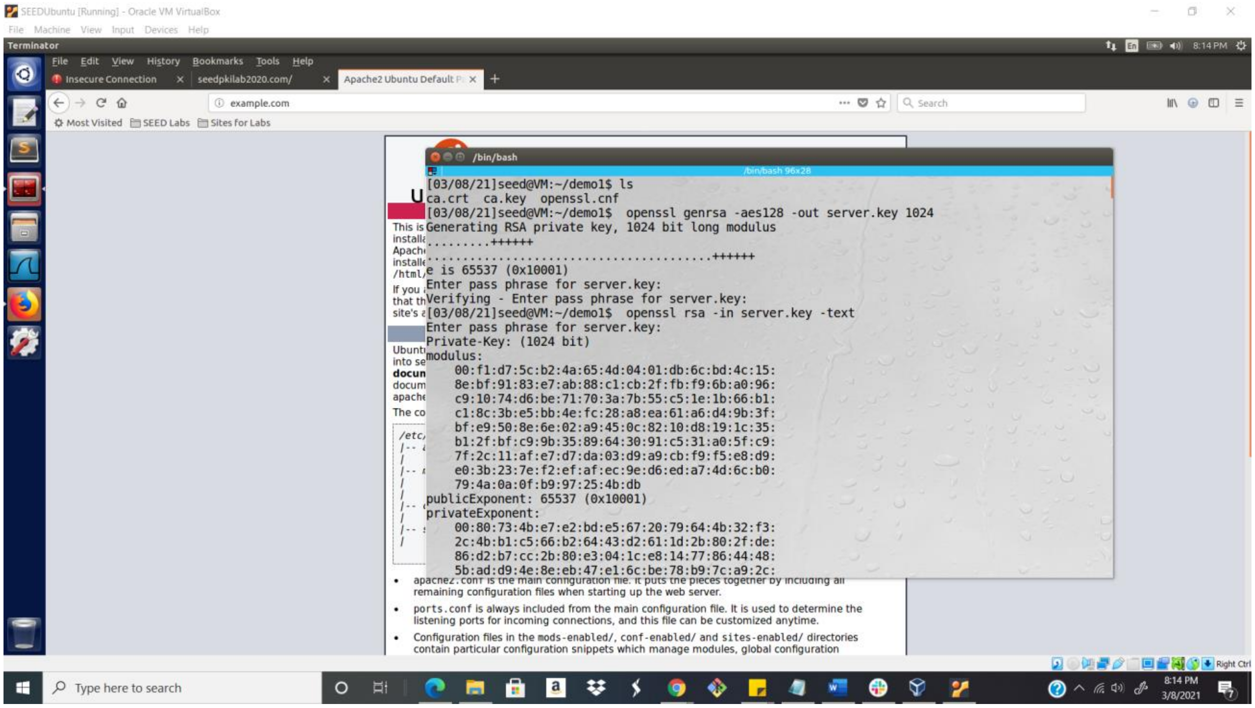
We can assume that the attacker can learn any long term aspect of your cipher implementation, such as the cipher name, mode of operation, key length. There are a number of possible ways they might learn it, such as an employee accidentally (or deliberately) leaking it, or if the attacker just obtains your implementation and dissects it. Hence, for security, we want to depend solely on something that we update routinely (such as the key). If the attacker learns the key, that limits the damage (as they can decrypt the traffic encrypted with that key, but nothing after we update the key). This idea is referred to as Kerckhoff's principle.

Now, you list the IV; that is typically updated constantly. On the other hand, we generally use it to refer to information that need not be secret. If it does have to be secret, then it really is part of the key, and should be considered that way.

Part-2 Assignments Lab:

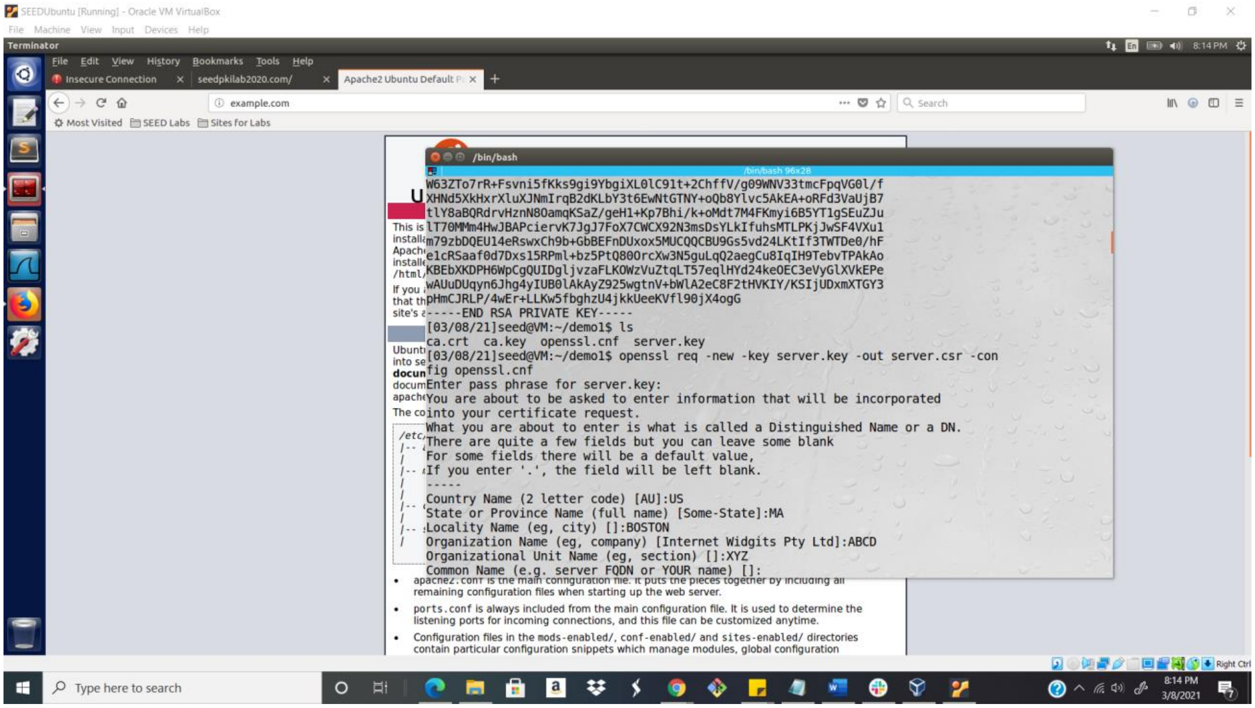
Public-Key Infrastructure (PKI) Lab

Enclosing all the screenshots of the SEED Lab Assignment on Ubuntu VM machine:



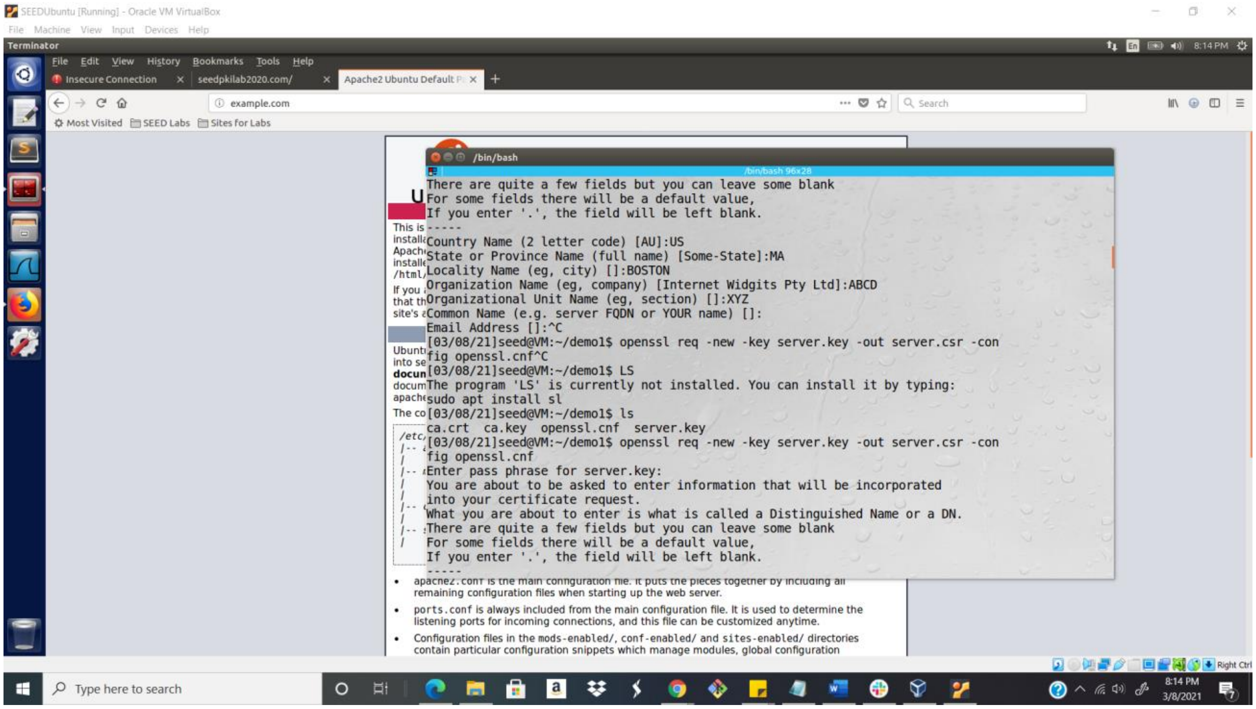
```
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  openssl.cnf
[03/08/21]seed@VM:~/demo1$  openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
.........++++++
.......................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[03/08/21]seed@VM:~/demo1$  openssl rsa -in server.key -text
Enter pass phrase for server.key:
Private-Key: (1024 bit)
modulus:
    00:f1:d7:5c:b2:4a:65:4d:04:01:db:6c:bd:4c:15:
    8e:bf:91:83:e7:ab:88:c1:cb:2f:fb:f9:6b:a0:96:
    c9:10:74:d6:be:71:70:3a:7b:55:c5:1e:1b:66:b1:
    c1:8c:3b:e5:bb:4e:fc:28:a8:ea:61:a6:d4:9b:3f:
    bf:e9:50:8e:6e:02:a9:45:0c:82:10:d8:19:1c:35:
    b1:2f:bf:c9:9b:35:89:64:30:91:c5:31:a0:5f:c9:
    7f:2c:11:af:e7:d7:da:03:d9:a9:cb:f9:f5:e8:d9:
    e0:3b:23:7e:f2:ef:af:ec:9e:d6:ed:a7:4d:6c:b0:
    79:4a:0a:0f:b9:97:25:4b:db
publicExponent: 65537 (0x10001)
privateExponent:
    00:80:73:4b:e7:e2:bd:e5:67:20:79:64:4b:32:f3:
    2c:4b:b1:c5:66:b2:64:43:d2:61:1d:2b:80:2f:de:
    86:d2:b7:cc:2b:80:e3:04:1c:e8:14:77:86:44:48:
    5b:ad:d9:4e:8e:eb:47:e1:6c:be:78:b9:7c:a9:2c:
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



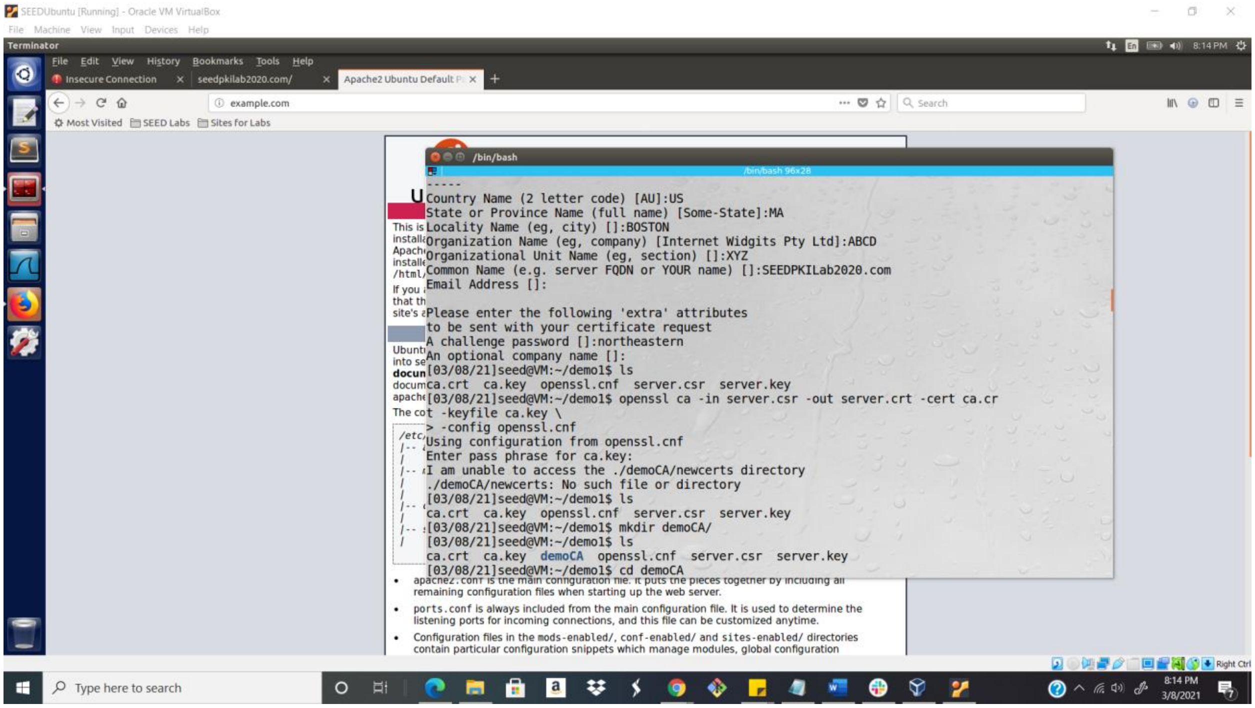
```
W63ZTo7rR+Fsvni5fKks9gi9YbgiXL0lC91t+2ChffV/g09WNV33tmcFpqVG0l/f
XHNd5XkHxrXluXJNmIrqB2dKLbY3t6EwNtGTNY+oQb8Ylvc5AkEA+oRFd3VaUjB7
tlY8aBQRdrvHznN8OamqKSaZ/geH1+Kp7Bhi/k+oMdt7M4FKmyi6B5YT1gSEuZJu
lT70MMm4HwJBAPciervK7JgJ7FoX7CWCX92N3msDsYLkIfuhsMTLPKjJwSF4VXu1
m79zbDQEU14eRswxCh9b+GbBEFnDUxox5MUCQQCBU9Gs5vd24LKtIf3TWTDe0/hF
e1cRSaaf0d7Dxs15RPml+bz5PtQ80OrcXw3N5guLqQ2aegCu8IqIH9TebvTPAkAo
KBEbXKDPH6WpCgQUIDgljvzaFLKOWzVuZtqLT57eqlHYd24keOEC3eVyGlXVkEPe
wAUuDUqyn6Jhg4yIUB0lAkAyZ925wgtnV+bWlA2eC8F2tHVKIY/KSIjUDxmXTGY3
pHmCJRLP/4wEr+LLKw5fbghzU4jkkUeeKVfl90jX4ogG
-----END RSA PRIVATE KEY-----
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  openssl.cnf  server.key
[03/08/21]seed@VM:~/demo1$ openssl req -new -key server.key -out server.csr -con
fig openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MA
Locality Name (eg, city) []:BOSTON
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABCD
Organizational Unit Name (eg, section) []:XYZ
Common Name (e.g. server FQDN or YOUR name) []:
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



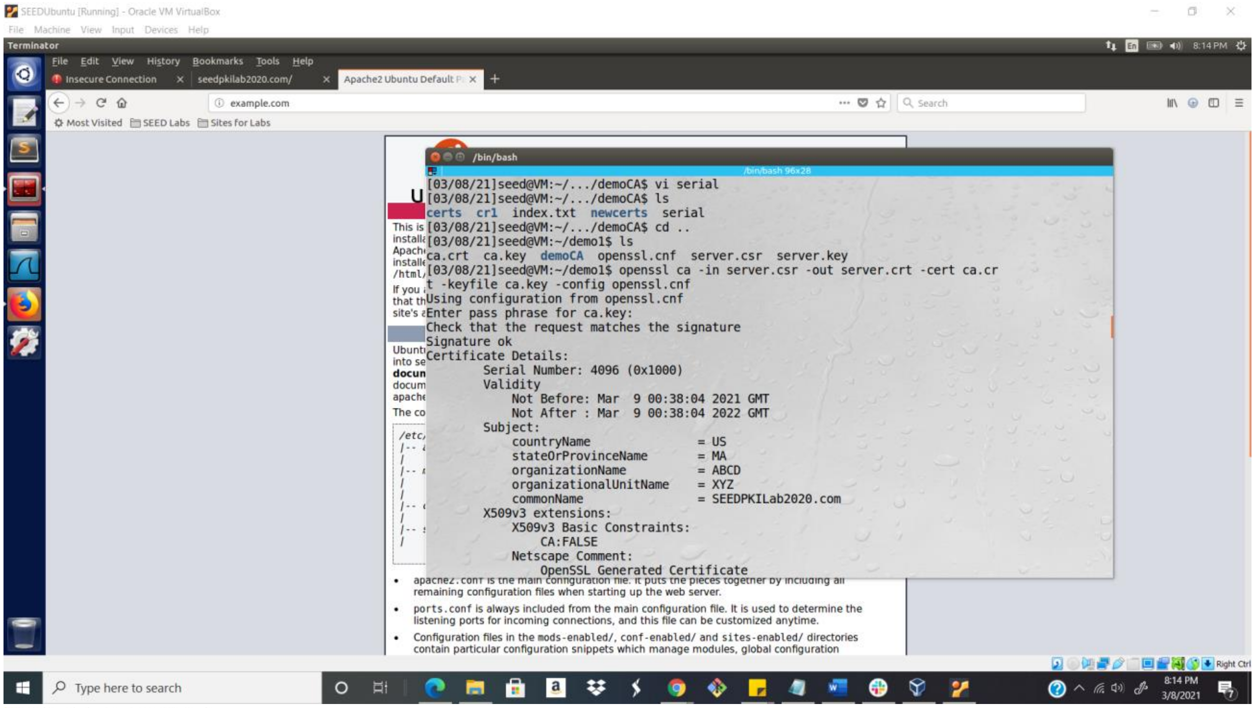
```
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MA
Locality Name (eg, city) []:BOSTON
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABCD
Organizational Unit Name (eg, section) []:XYZ
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:^C
[03/08/21]seed@VM:~/demo1$ openssl req -new -key server.key -out server.csr -con
fig openssl.cnf^C
[03/08/21]seed@VM:~/demo1$ LS
The program 'LS' is currently not installed. You can install it by typing:
sudo apt install sl
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  openssl.cnf  server.key
[03/08/21]seed@VM:~/demo1$ openssl req -new -key server.key -out server.csr -con
fig openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



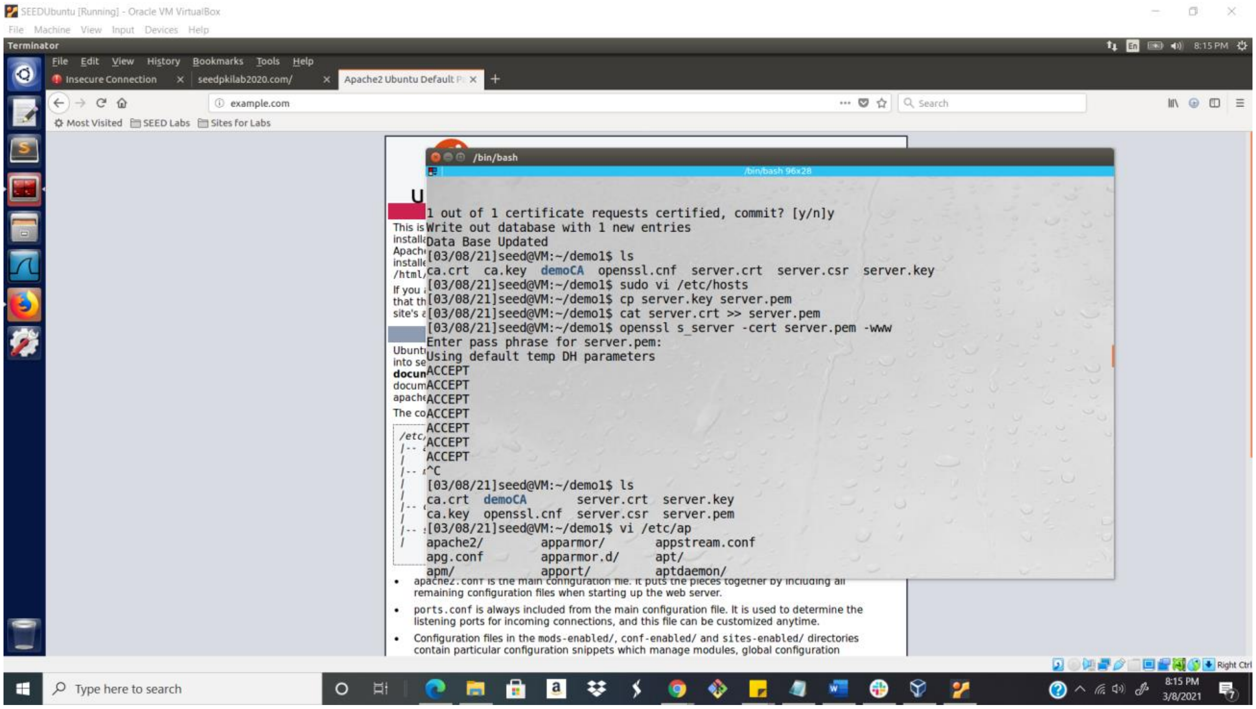
```
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:MA
Locality Name (eg, city) []:BOSTON
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABCD
Organizational Unit Name (eg, section) []:XYZ
Common Name (e.g. server FQDN or YOUR name) []:SEEDPKILab2020.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:northeastern
An optional company name []:
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  openssl.cnf  server.csr  server.key
[03/08/21]seed@VM:~/demo1$ openssl ca -in server.csr -out server.crt -cert ca.cr
t -keyfile ca.key \
> -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
I am unable to access the ./demoCA/newcerts directory
./demoCA/newcerts: No such file or directory
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  openssl.cnf  server.csr  server.key
[03/08/21]seed@VM:~/demo1$ mkdir demoCA/
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  demoCA  openssl.cnf  server.csr  server.key
[03/08/21]seed@VM:~/demo1$ cd demoCA
```

- remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



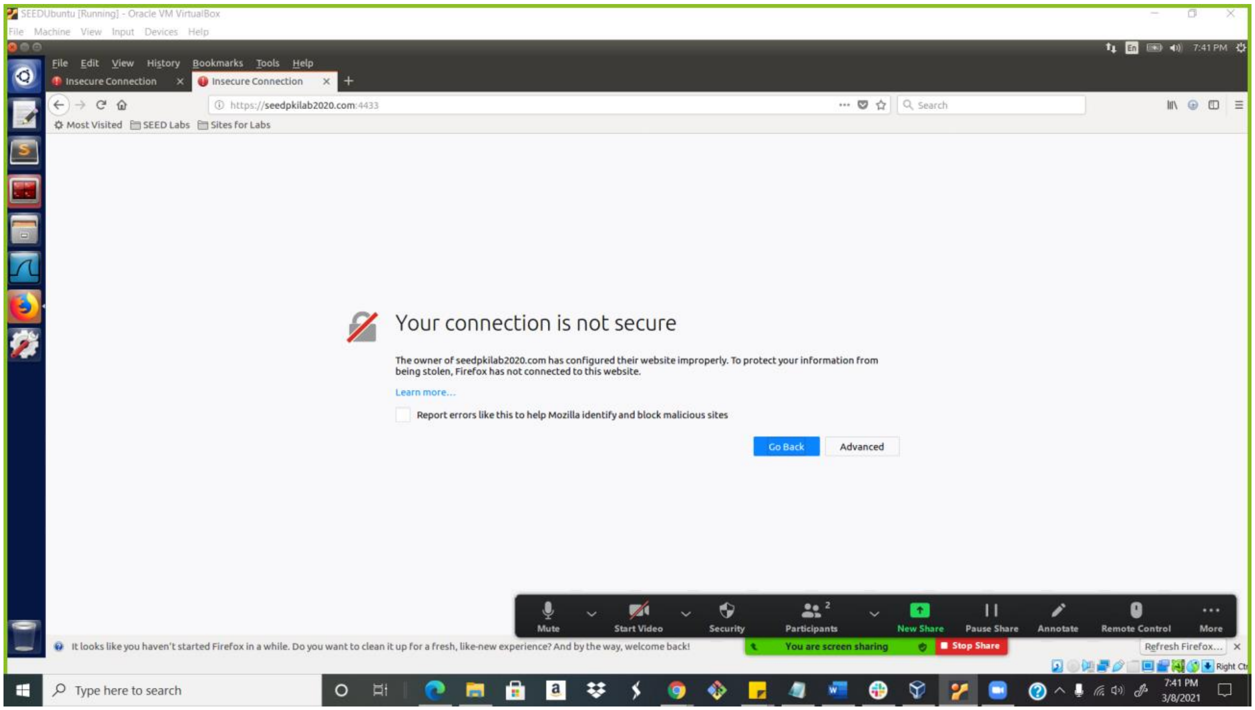
```
[03/08/21]seed@VM:~/.../demoCA$ vi serial
[03/08/21]seed@VM:~/.../demoCA$ ls
certs  crl  index.txt  newcerts  serial
[03/08/21]seed@VM:~/.../demoCA$ cd ..
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  demoCA  openssl.cnf  server.csr  server.key
[03/08/21]seed@VM:~/demo1$ openssl ca -in server.csr -out server.crt -cert ca.cr
t -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Mar  9 00:38:04 2021 GMT
            Not After : Mar  9 00:38:04 2022 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = MA
            organizationName          = ABCD
            organizationalUnitName    = XYZ
            commonName                = SEEDPKILab2020.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
```

- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



```
1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  ca.key  demoCA  openssl.cnf  server.crt  server.csr  server.key
[03/08/21]seed@VM:~/demo1$ sudo vi /etc/hosts
[03/08/21]seed@VM:~/demo1$ cp server.key server.pem
[03/08/21]seed@VM:~/demo1$ cat server.crt >> server.pem
[03/08/21]seed@VM:~/demo1$ openssl s_server -cert server.pem -www
Enter pass phrase for server.pem:
Using default temp DH parameters
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
ACCEPT
^C
[03/08/21]seed@VM:~/demo1$ ls
ca.crt  demoCA       server.crt  server.key
ca.key  openssl.cnf  server.csr  server.pem
[03/08/21]seed@VM:~/demo1$ vi /etc/ap
apache2/        apparmor/       appstream.conf
apg.conf        apparmor.d/     apt/
apm/            apport/         aptdaemon/
```

- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



Your connection is not secure

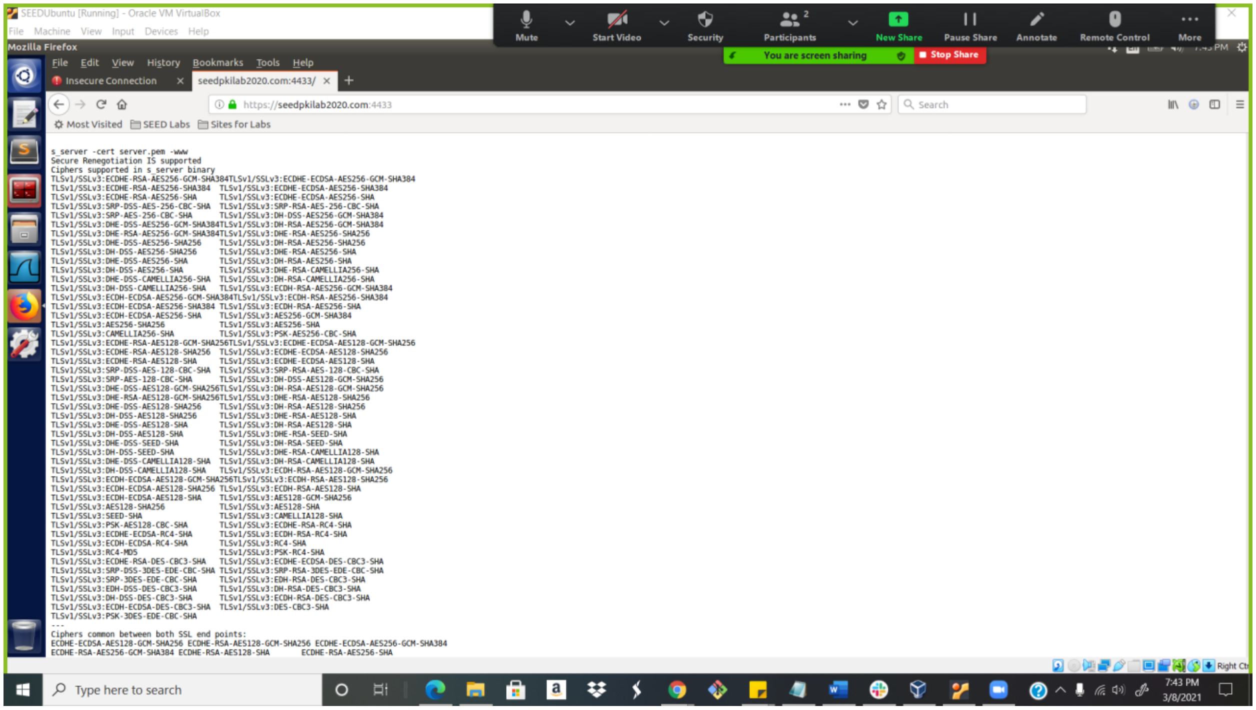
The owner of seedpkilab2020.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

Learn more…

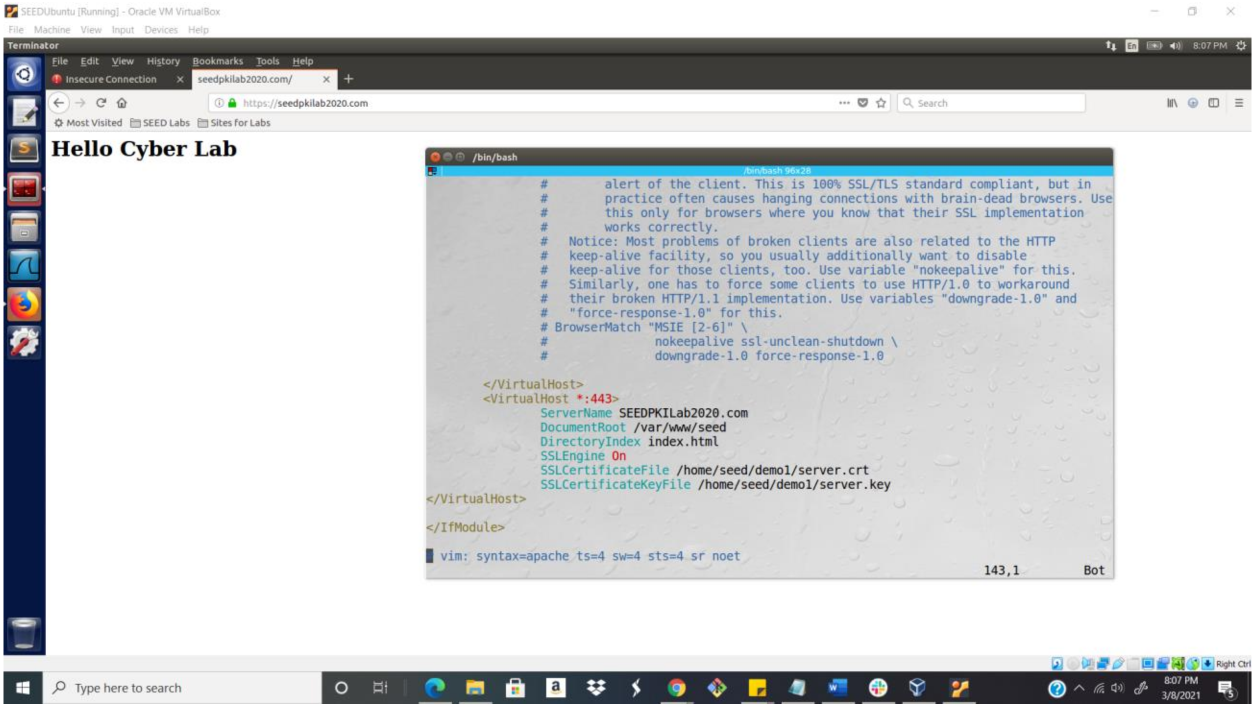
□ Report errors like this to help Mozilla identify and block malicious sites

Go Back   Advanced

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

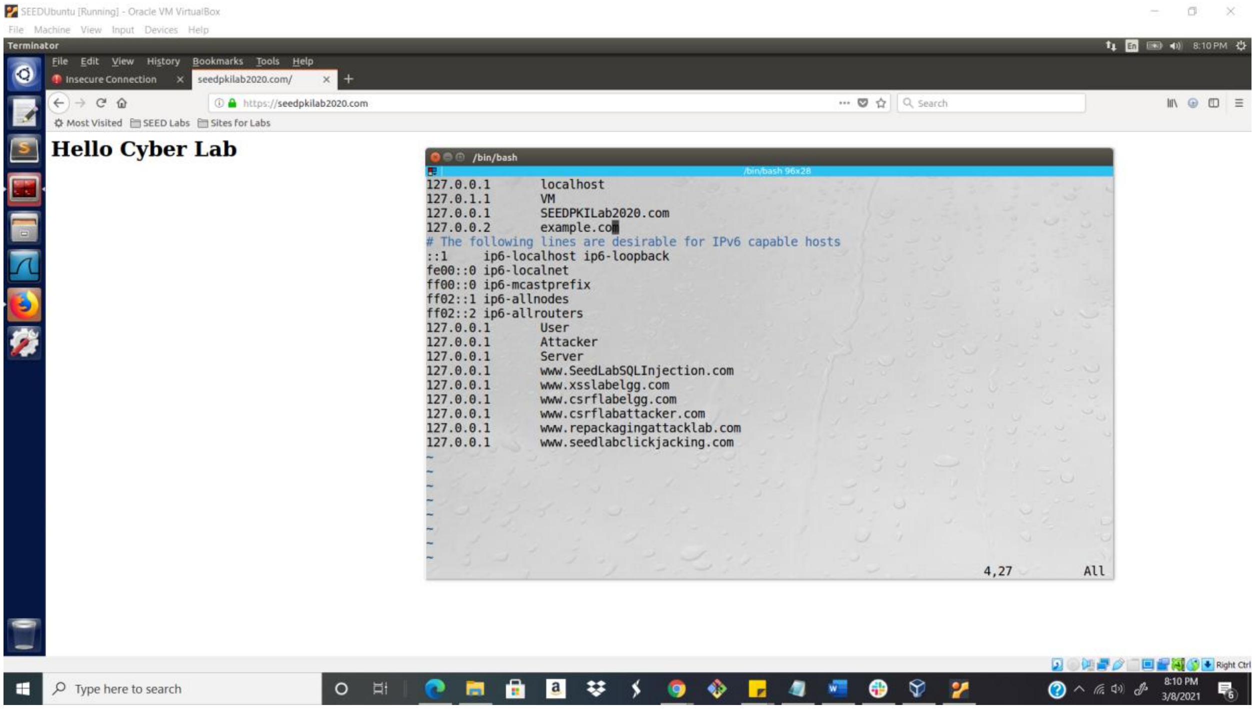


```
s_server -cert server.pem -www
Secure Renegotiation IS supported
Ciphers supported in s_server binary
TLSv1/SSLv3:ECDHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDHE-ECDSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA384  TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA384
TLSv1/SSLv3:ECDHE-RSA-AES256-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES256-SHA
TLSv1/SSLv3:SRP-DSS-AES-256-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-256-CBC-SHA
TLSv1/SSLv3:SRP-AES-256-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-DSS-AES256-GCM-SHA384TLSv1/SSLv3:DH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:DHE-RSA-AES256-GCM-SHA384TLSv1/SSLv3:DHE-RSA-AES256-SHA256
TLSv1/SSLv3:DHE-DSS-AES256-SHA256    TLSv1/SSLv3:DH-RSA-AES256-SHA256
TLSv1/SSLv3:DH-DSS-AES256-SHA256     TLSv1/SSLv3:DHE-RSA-AES256-SHA
TLSv1/SSLv3:DHE-DSS-AES256-SHA       TLSv1/SSLv3:DH-RSA-AES256-SHA
TLSv1/SSLv3:DH-DSS-AES256-SHA        TLSv1/SSLv3:DHE-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA256-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA256-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA256-SHA   TLSv1/SSLv3:ECDH-RSA-AES256-GCM-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-GCM-SHA384TLSv1/SSLv3:ECDH-RSA-AES256-SHA384
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA384 TLSv1/SSLv3:ECDH-RSA-AES256-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES256-SHA    TLSv1/SSLv3:AES256-GCM-SHA384
TLSv1/SSLv3:AES256-SHA256            TLSv1/SSLv3:AES256-SHA
TLSv1/SSLv3:CAMELLIA256-SHA          TLSv1/SSLv3:PSK-AES256-CBC-SHA
TLSv1/SSLv3:ECDHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDHE-ECDSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA256  TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA256
TLSv1/SSLv3:ECDHE-RSA-AES128-SHA     TLSv1/SSLv3:ECDHE-ECDSA-AES128-SHA
TLSv1/SSLv3:SRP-DSS-AES-128-CBC-SHA  TLSv1/SSLv3:SRP-RSA-AES-128-CBC-SHA
TLSv1/SSLv3:SRP-AES-128-CBC-SHA      TLSv1/SSLv3:DH-DSS-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-GCM-SHA256TLSv1/SSLv3:DH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:DHE-RSA-AES128-GCM-SHA256TLSv1/SSLv3:DHE-RSA-AES128-SHA256
TLSv1/SSLv3:DHE-DSS-AES128-SHA256    TLSv1/SSLv3:DH-RSA-AES128-SHA256
TLSv1/SSLv3:DH-DSS-AES128-SHA256     TLSv1/SSLv3:DHE-RSA-AES128-SHA
TLSv1/SSLv3:DHE-DSS-AES128-SHA       TLSv1/SSLv3:DH-RSA-AES128-SHA
TLSv1/SSLv3:DH-DSS-AES128-SHA        TLSv1/SSLv3:DHE-RSA-SEED-SHA
TLSv1/SSLv3:DHE-DSS-SEED-SHA         TLSv1/SSLv3:DH-RSA-SEED-SHA
TLSv1/SSLv3:DH-DSS-SEED-SHA          TLSv1/SSLv3:DHE-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DHE-DSS-CAMELLIA128-SHA  TLSv1/SSLv3:DH-RSA-CAMELLIA128-SHA
TLSv1/SSLv3:DH-DSS-CAMELLIA128-SHA   TLSv1/SSLv3:ECDH-RSA-AES128-GCM-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-GCM-SHA256TLSv1/SSLv3:ECDH-RSA-AES128-SHA256
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA256 TLSv1/SSLv3:ECDH-RSA-AES128-SHA
TLSv1/SSLv3:ECDH-ECDSA-AES128-SHA    TLSv1/SSLv3:AES128-GCM-SHA256
TLSv1/SSLv3:AES128-SHA256            TLSv1/SSLv3:AES128-SHA
TLSv1/SSLv3:SEED-SHA                 TLSv1/SSLv3:CAMELLIA128-SHA
TLSv1/SSLv3:PSK-AES128-CBC-SHA       TLSv1/SSLv3:ECDHE-RSA-RC4-SHA
TLSv1/SSLv3:ECDHE-ECDSA-RC4-SHA      TLSv1/SSLv3:ECDH-RSA-RC4-SHA
TLSv1/SSLv3:ECDH-ECDSA-RC4-SHA       TLSv1/SSLv3:RC4-SHA
TLSv1/SSLv3:RC4-MD5                  TLSv1/SSLv3:PSK-RC4-SHA
TLSv1/SSLv3:ECDHE-RSA-DES-CBC3-SHA   TLSv1/SSLv3:ECDHE-ECDSA-DES-CBC3-SHA
TLSv1/SSLv3:SRP-DSS-3DES-EDE-CBC-SHA TLSv1/SSLv3:SRP-RSA-3DES-EDE-CBC-SHA
TLSv1/SSLv3:SRP-3DES-EDE-CBC-SHA     TLSv1/SSLv3:EDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:EDH-DSS-DES-CBC3-SHA     TLSv1/SSLv3:DH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:DH-DSS-DES-CBC3-SHA      TLSv1/SSLv3:ECDH-RSA-DES-CBC3-SHA
TLSv1/SSLv3:ECDH-ECDSA-DES-CBC3-SHA  TLSv1/SSLv3:DES-CBC3-SHA
TLSv1/SSLv3:PSK-3DES-EDE-CBC-SHA
---
Ciphers common between both SSL end points:
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA       ECDHE-RSA-AES256-SHA
```



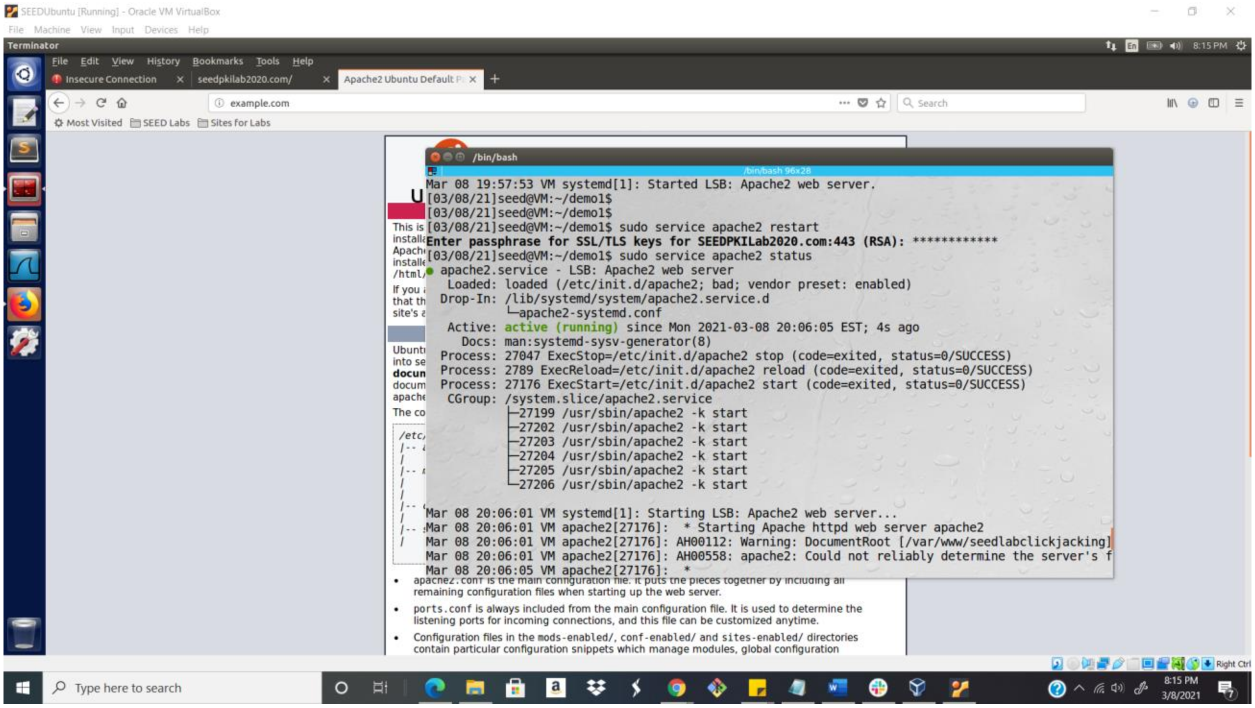
Hello Cyber Lab

```
                #       alert of the client. This is 100% SSL/TLS standard compliant, but in
                #       practice often causes hanging connections with brain-dead browsers. Use
                #       this only for browsers where you know that their SSL implementation
                #       works correctly.
                #   Notice: Most problems of broken clients are also related to the HTTP
                #   keep-alive facility, so you usually additionally want to disable
                #   keep-alive for those clients, too. Use variable "nokeepalive" for this.
                #   Similarly, one has to force some clients to use HTTP/1.0 to workaround
                #   their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
                #   "force-response-1.0" for this.
                # BrowserMatch "MSIE [2-6]" \
                #               nokeepalive ssl-unclean-shutdown \
                #               downgrade-1.0 force-response-1.0

        </VirtualHost>
        <VirtualHost *:443>
                ServerName SEEDPKILab2020.com
                DocumentRoot /var/www/seed
                DirectoryIndex index.html
                SSLEngine On
                SSLCertificateFile /home/seed/demo1/server.crt
                SSLCertificateKeyFile /home/seed/demo1/server.key
</VirtualHost>

</IfModule>

 vim: syntax=apache ts=4 sw=4 sts=4 sr noet
                                                                                143,1         Bot
```



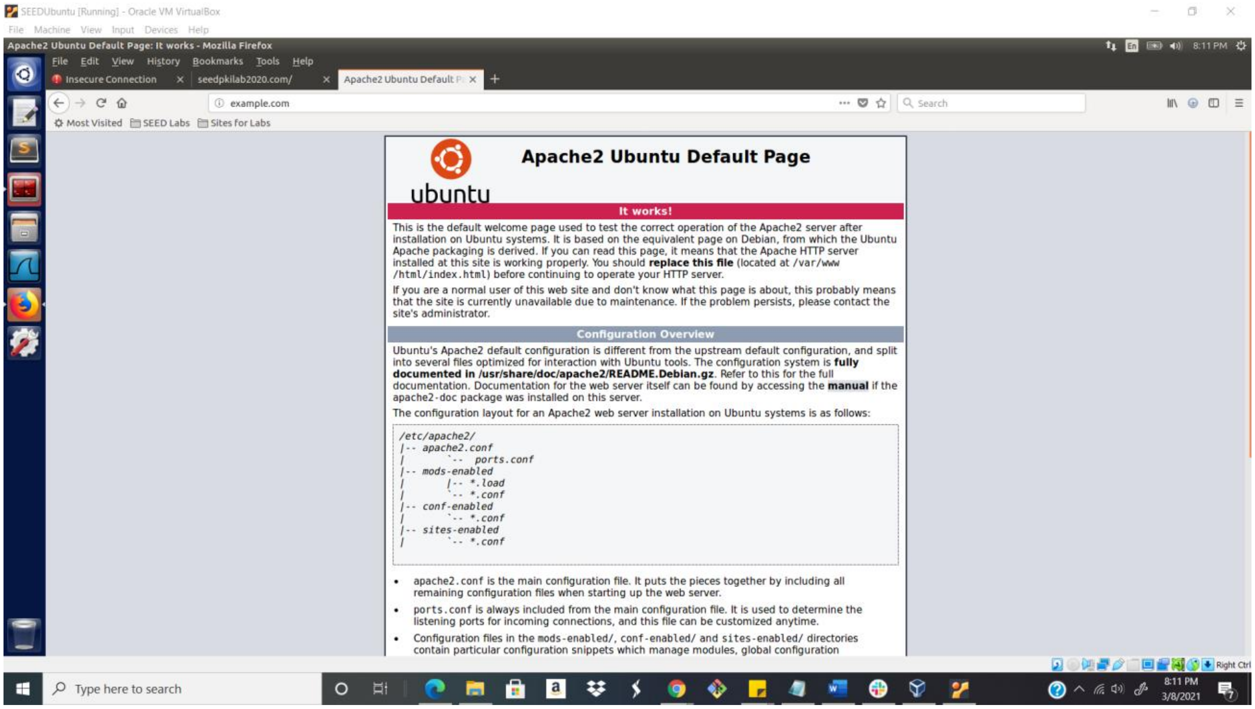
Hello Cyber Lab

```
127.0.0.1       localhost
127.0.1.1       VM
127.0.0.1       SEEDPKILab2020.com
127.0.0.2       example.com
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
127.0.0.1       User
127.0.0.1       Attacker
127.0.0.1       Server
127.0.0.1       www.SeedLabSQLInjection.com
127.0.0.1       www.xsslabelgg.com
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
~
~
~
~
~
~
~
~
                                                                                4,27          All
```



```
Mar 08 19:57:53 VM systemd[1]: Started LSB: Apache2 web server.
[03/08/21]seed@VM:~/demo1$
[03/08/21]seed@VM:~/demo1$
[03/08/21]seed@VM:~/demo1$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2020.com:443 (RSA): ************
[03/08/21]seed@VM:~/demo1$ sudo service apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Mon 2021-03-08 20:06:05 EST; 4s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 27047 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)
  Process: 2789 ExecReload=/etc/init.d/apache2 reload (code=exited, status=0/SUCCESS)
  Process: 27176 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/apache2.service
           ├─27199 /usr/sbin/apache2 -k start
           ├─27202 /usr/sbin/apache2 -k start
           ├─27203 /usr/sbin/apache2 -k start
           ├─27204 /usr/sbin/apache2 -k start
           ├─27205 /usr/sbin/apache2 -k start
           └─27206 /usr/sbin/apache2 -k start

Mar 08 20:06:01 VM systemd[1]: Starting LSB: Apache2 web server...
Mar 08 20:06:01 VM apache2[27176]:  * Starting Apache httpd web server apache2
Mar 08 20:06:01 VM apache2[27176]: AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking]
Mar 08 20:06:01 VM apache2[27176]: AH00558: apache2: Could not reliably determine the server's f
Mar 08 20:06:05 VM apache2[27176]:  *
```

- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration


SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Apache2 Ubuntu Default Page: It works - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Insecure Connection
seedpkilab2020.com/
Apache2 Ubuntu Default P
example.com
Search
Most Visited
SEED Labs
Sites for Labs
ubuntu
Type here to search
8:11 PM
3/8/2021

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

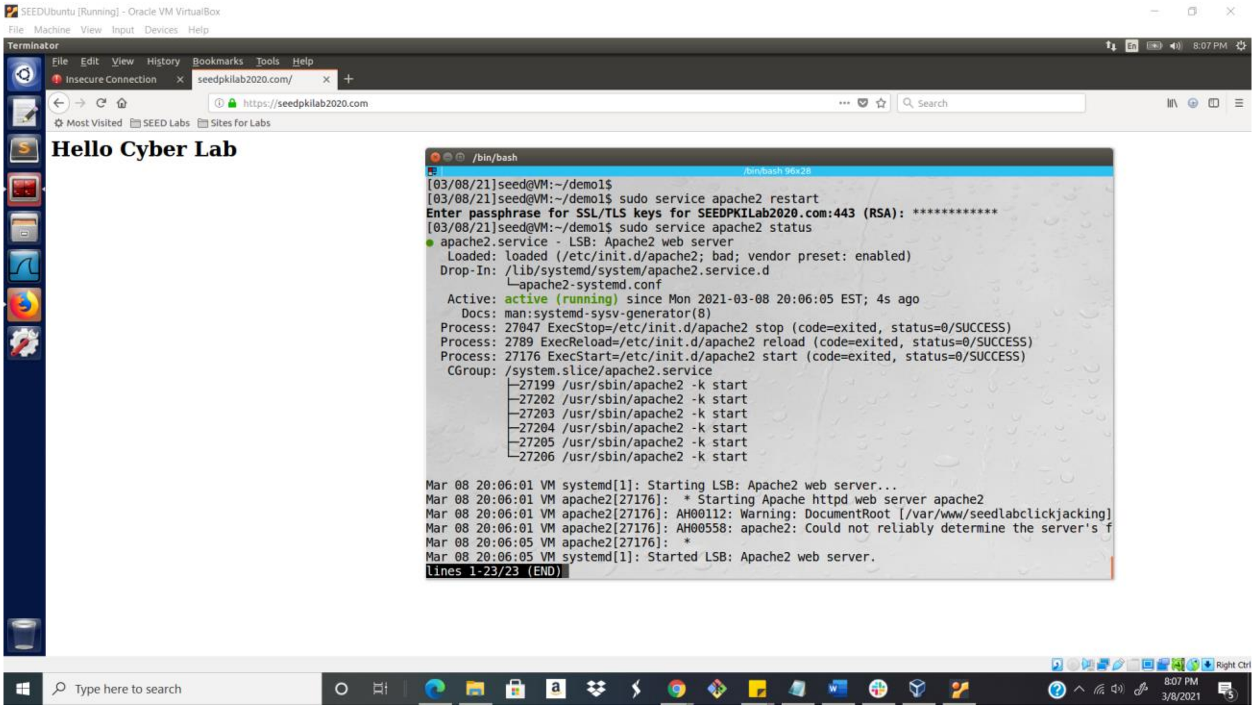
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

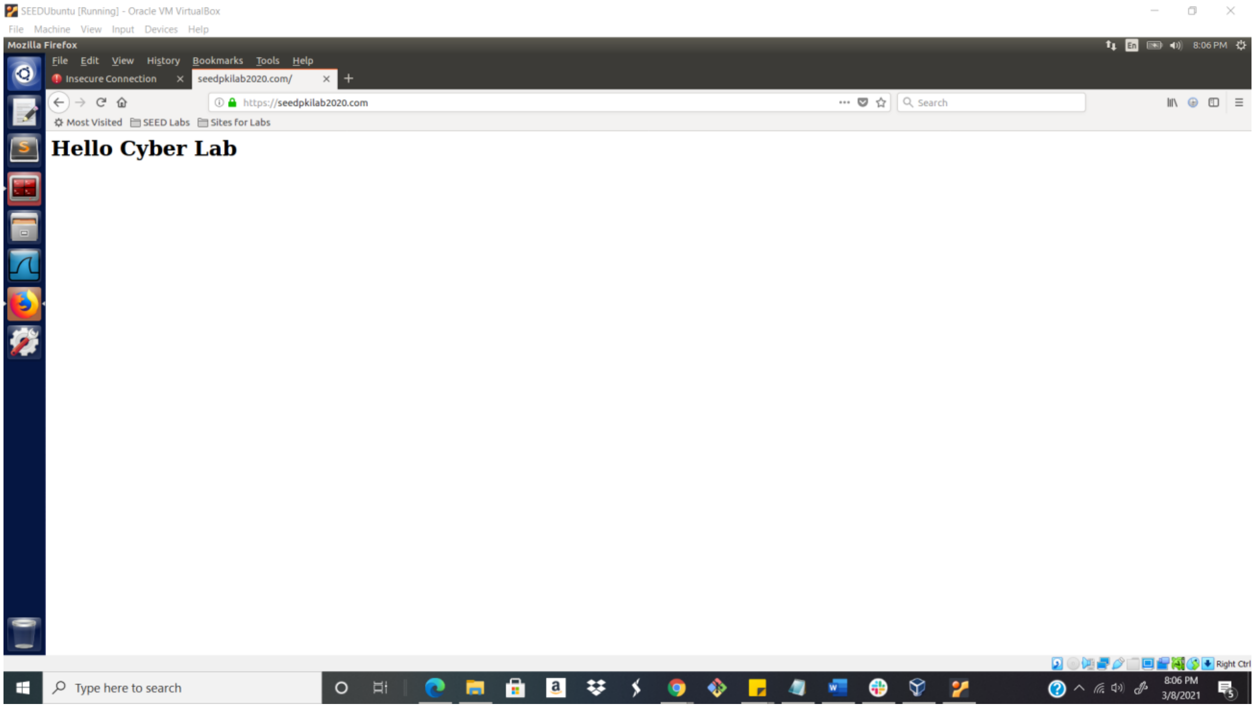
```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration



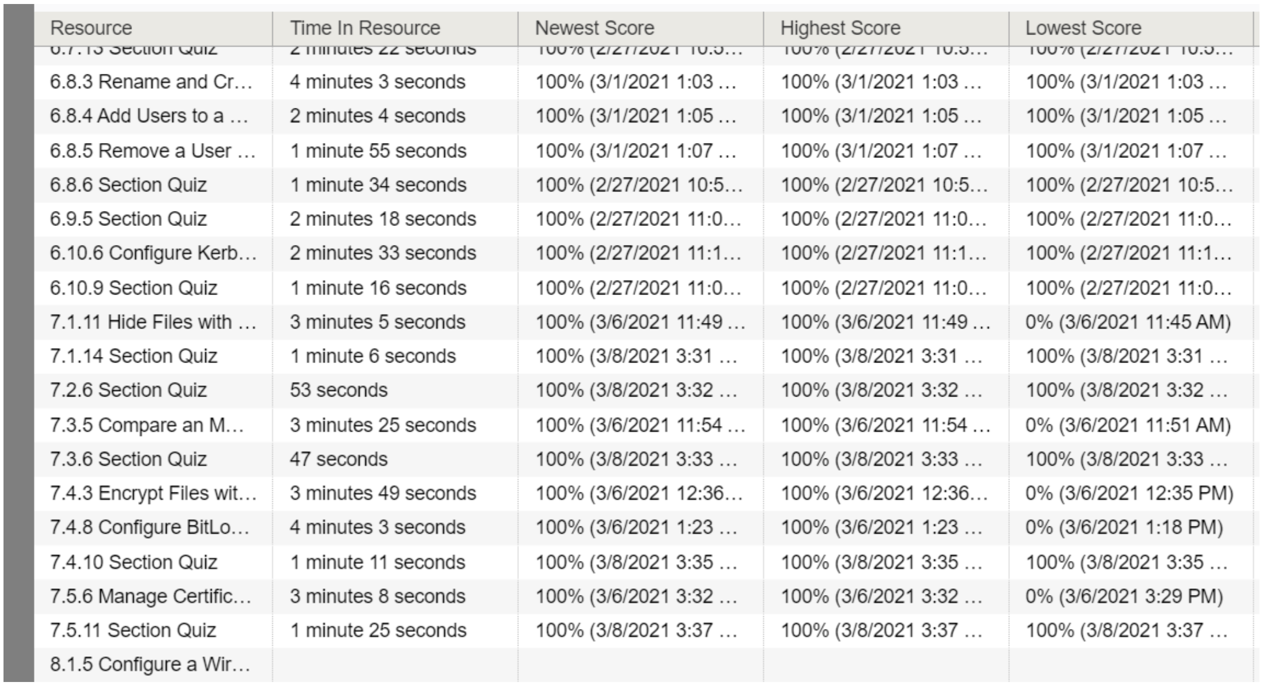
Hello Cyber Lab

```
[03/08/21]seed@VM:~/demo1$
[03/08/21]seed@VM:~/demo1$ sudo service apache2 restart
Enter passphrase for SSL/TLS keys for SEEDPKILab2020.com:443 (RSA): ************
[03/08/21]seed@VM:~/demo1$ sudo service apache2 status
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2; bad; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Mon 2021-03-08 20:06:05 EST; 4s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 27047 ExecStop=/etc/init.d/apache2 stop (code=exited, status=0/SUCCESS)
  Process: 2789 ExecReload=/etc/init.d/apache2 reload (code=exited, status=0/SUCCESS)
  Process: 27176 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/apache2.service
           ├─27199 /usr/sbin/apache2 -k start
           ├─27202 /usr/sbin/apache2 -k start
           ├─27203 /usr/sbin/apache2 -k start
           ├─27204 /usr/sbin/apache2 -k start
           ├─27205 /usr/sbin/apache2 -k start
           └─27206 /usr/sbin/apache2 -k start

Mar 08 20:06:01 VM systemd[1]: Starting LSB: Apache2 web server...
Mar 08 20:06:01 VM apache2[27176]:  * Starting Apache httpd web server apache2
Mar 08 20:06:01 VM apache2[27176]: AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking]
Mar 08 20:06:01 VM apache2[27176]: AH00558: apache2: Could not reliably determine the server's f
Mar 08 20:06:05 VM apache2[27176]:  *
Mar 08 20:06:05 VM systemd[1]: Started LSB: Apache2 web server.
lines 1-23/23 (END)
```


SEEDUbuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mozilla Firefox
8:06 PM
File Edit View History Bookmarks Tools Help
Insecure Connection
seedpkilab2020.com/
https://seedpkilab2020.com
Search
Most Visited
SEED Labs
Sites for Labs
Right Ctrl
Type here to search
8:06 PM
3/8/2021

Hello Cyber Lab

Progress Embedded Image of Progress Report from LabSim:



Resource	Time In Resource	Newest Score	Highest Score	Lowest Score
6.7.13 Section Quiz	2 minutes 22 seconds	100% (2/27/2021 10:5…	100% (2/27/2021 10:5…	100% (2/27/2021 10:5…
6.8.3 Rename and Cr…	4 minutes 3 seconds	100% (3/1/2021 1:03 …	100% (3/1/2021 1:03 …	100% (3/1/2021 1:03 …
6.8.4 Add Users to a …	2 minutes 4 seconds	100% (3/1/2021 1:05 …	100% (3/1/2021 1:05 …	100% (3/1/2021 1:05 …
6.8.5 Remove a User …	1 minute 55 seconds	100% (3/1/2021 1:07 …	100% (3/1/2021 1:07 …	100% (3/1/2021 1:07 …
6.8.6 Section Quiz	1 minute 34 seconds	100% (2/27/2021 10:5…	100% (2/27/2021 10:5…	100% (2/27/2021 10:5…
6.9.5 Section Quiz	2 minutes 18 seconds	100% (2/27/2021 11:0…	100% (2/27/2021 11:0…	100% (2/27/2021 11:0…
6.10.6 Configure Kerb…	2 minutes 33 seconds	100% (2/27/2021 11:1…	100% (2/27/2021 11:1…	100% (2/27/2021 11:1…
6.10.9 Section Quiz	1 minute 16 seconds	100% (2/27/2021 11:0…	100% (2/27/2021 11:0…	100% (2/27/2021 11:0…
7.1.11 Hide Files with …	3 minutes 5 seconds	100% (3/6/2021 11:49 …	100% (3/6/2021 11:49 …	0% (3/6/2021 11:45 AM)
7.1.14 Section Quiz	1 minute 6 seconds	100% (3/8/2021 3:31 …	100% (3/8/2021 3:31 …	100% (3/8/2021 3:31 …
7.2.6 Section Quiz	53 seconds	100% (3/8/2021 3:32 …	100% (3/8/2021 3:32 …	100% (3/8/2021 3:32 …
7.3.5 Compare an M…	3 minutes 25 seconds	100% (3/6/2021 11:54 …	100% (3/6/2021 11:54 …	0% (3/6/2021 11:51 AM)
7.3.6 Section Quiz	47 seconds	100% (3/8/2021 3:33 …	100% (3/8/2021 3:33 …	100% (3/8/2021 3:33 …
7.4.3 Encrypt Files wit…	3 minutes 49 seconds	100% (3/6/2021 12:36…	100% (3/6/2021 12:36…	0% (3/6/2021 12:35 PM)
7.4.8 Configure BitLo…	4 minutes 3 seconds	100% (3/6/2021 1:23 …	100% (3/6/2021 1:23 …	0% (3/6/2021 1:18 PM)
7.4.10 Section Quiz	1 minute 11 seconds	100% (3/8/2021 3:35 …	100% (3/8/2021 3:35 …	100% (3/8/2021 3:35 …
7.5.6 Manage Certific…	3 minutes 8 seconds	100% (3/6/2021 3:32 …	100% (3/6/2021 3:32 …	0% (3/6/2021 3:29 PM)
7.5.11 Section Quiz	1 minute 25 seconds	100% (3/8/2021 3:37 …	100% (3/8/2021 3:37 …	100% (3/8/2021 3:37 …
8.1.5 Configure a Wir…				