COMP3052 Computer Security

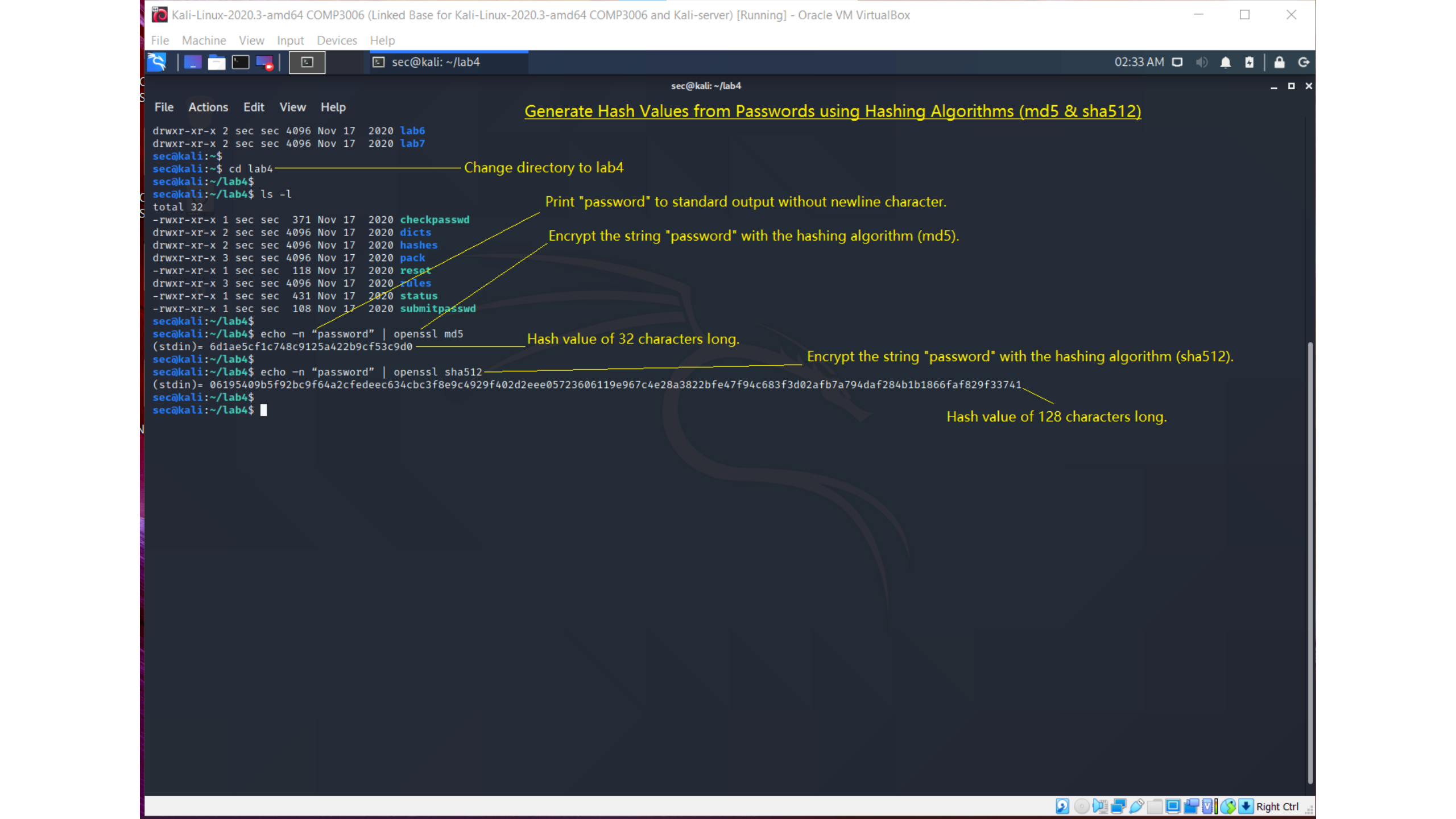
Session 02: Motivating Example

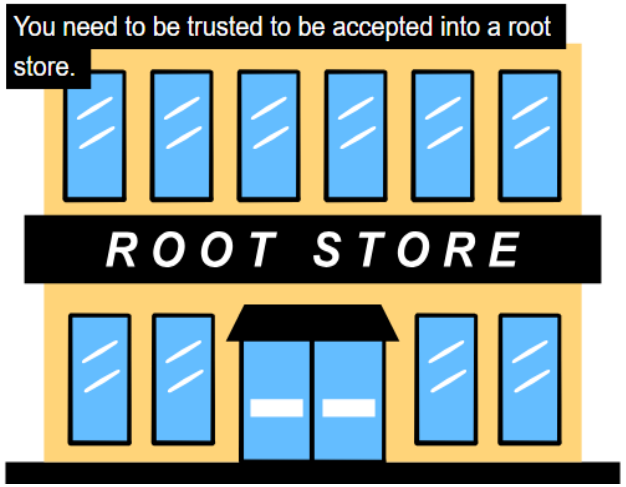
Videoclip: Key Exchange

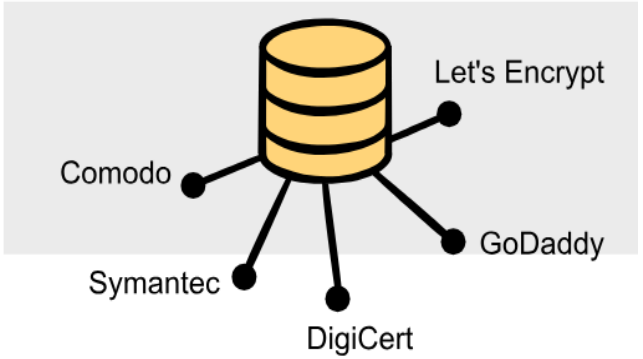
https://www.youtube.com/watch?v=U62S8SchxX4

Videoclip: How Encryption Keys Work - with Chris Bishop

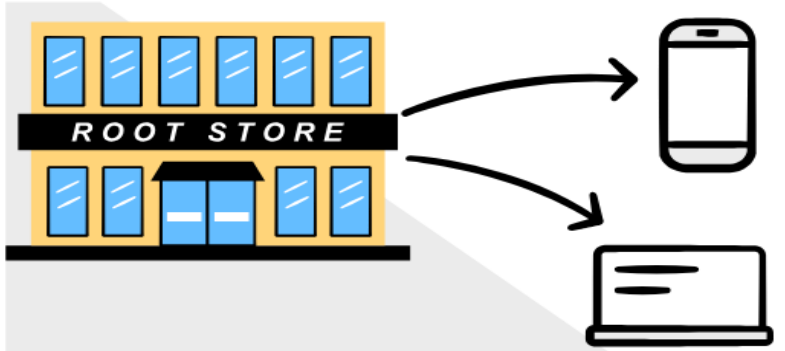
https://www.youtube.com/watch?v=EDTx3meIeT0


Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-server) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~/lab4
02:33 AM
sec@kali: ~/lab4
File Actions Edit View Help
Generate Hash Values from Passwords using Hashing Algorithms (md5 & sha512)
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab6
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 lab7
sec@kali:~$
sec@kali:~$ cd lab4
Change directory to lab4
sec@kali:~/lab4$
sec@kali:~/lab4$ ls -l
total 32
-rwxr-xr-x 1 sec sec 371 Nov 17 2020 checkpasswd
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 dicts
drwxr-xr-x 2 sec sec 4096 Nov 17 2020 hashes
drwxr-xr-x 3 sec sec 4096 Nov 17 2020 pack
-rwxr-xr-x 1 sec sec 118 Nov 17 2020 reset
drwxr-xr-x 3 sec sec 4096 Nov 17 2020 rules
-rwxr-xr-x 1 sec sec 431 Nov 17 2020 status
-rwxr-xr-x 1 sec sec 108 Nov 17 2020 submitpasswd
Print "password" to standard output without newline character.
Encrypt the string "password" with the hashing algorithm (md5).
sec@kali:~/lab4$
sec@kali:~/lab4$ echo -n “password” | openssl md5
(stdin)= 6d1ae5cf1c748c9125a422b9cf53c9d0
Hash value of 32 characters long.
sec@kali:~/lab4$
sec@kali:~/lab4$ echo -n “password” | openssl sha512
Encrypt the string "password" with the hashing algorithm (sha512).
(stdin)= 06195409b5f92bc9f64a2cfedeec634cbc3f8e9c4929f402d2eee05723606119e967c4e28a3822bfe47f94c683f3d02afb7a794daf284b1b1866faf829f33741
Hash value of 128 characters long.
sec@kali:~/lab4$
sec@kali:~/lab4$
Right Ctrl

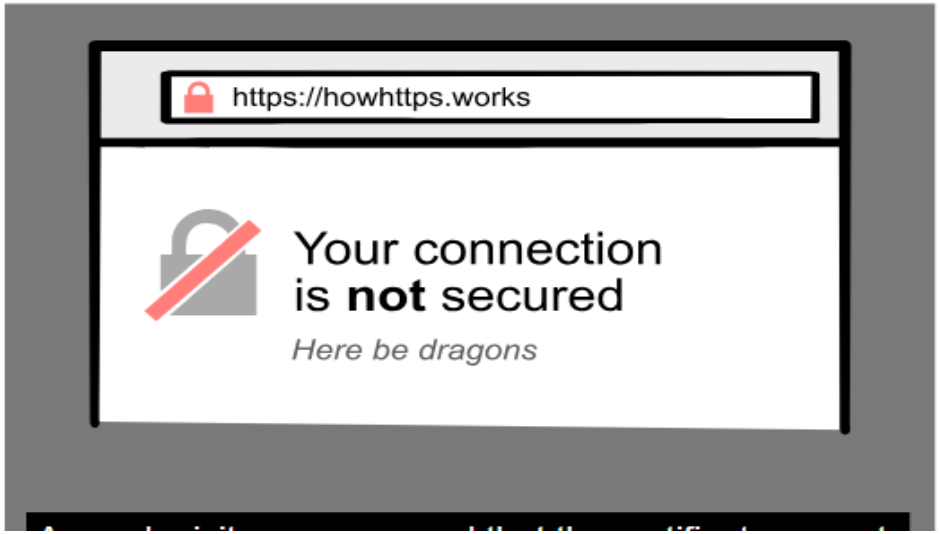




A root store is basically a database of trusted CAs.



Apple, Windows, and Mozilla run their own root stores that they pre-install in your computer or device.



Reference: Certificate Authorities

https://howhttps.works/certificate-authorities/

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ 08:24 AM

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$
sec@kali:~$ sudo -i
[sudo] password for sec:
root@kali:~#
root@kali:~#
root@kali:~# wget -O keyfile https://archive.kali.org/archive-key.asc
--2023-01-26 08:20:23--  https://archive.kali.org/archive-key.asc
Resolving archive.kali.org (archive.kali.org)... 192.99.45.140
Connecting to archive.kali.org (archive.kali.org)|192.99.45.140|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3155 (3.1K) [application/octet-stream]
Saving to: 'keyfile'

keyfile                          100%[===================================>]   3.08K  --.-KB/s    in 0s

2023-01-26 08:20:24 (88.6 MB/s) - 'keyfile' saved [3155/3155]

root@kali:~#
root@kali:~#
root@kali:~# cat keyfile
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBE9U1CgBEAChen9+cvBS8ioHoCU6wBbL9jaIk5P7ZkPpjDsovMvimqZaozS8
fEAZM23gJlFratc+rRllV9hPZmGqhtT50RLDzC3yFOvFnJqAPvpVDO2ipQCVnJDX
0eWDhT62RDwk+FhjksEDwP7Yc4CgohdGDYQu1zTBSLL5qen3rckCnHF2OnSiKnYM
8YCIKAYMt4VRArAvivjOMspN+1xy2S8GYXX2felsu3Ir1DXvUIE7b/9sdK6MzBcq
joDH34OqX6isqAW0+K93lmVN+U4yFMzfEB74UMQNWKg39mCB0K/VfQ89ih4zvF9a
zENbFzfF0O0h09oHF4ZTaUFeI8JImp/x9FC+LveUyJot9t/xv0HVUd08Y4PgO48C
iXOTqqqm/DPF0AbHJGpTuonOsKy3/dYhk7Fvsfn02DMds+RKsukBEzypTIIIzMBF
Uwiq/GaaNRWw6lnOyE4wMmpwRa11QVDDWkMpuOr1tPV7M+EMAhZY7cyHDmRTOFL3
H0CxYnInis+k1NQikqtLxNrzWdxsXU25BMbEsAQq7aRTs7wpOnUK+yY+qTG/V5nl
J6II+/CtWJthIef22r8EYX1BQOXRggamy0nxViC3S6kjuU2Lb1qnDb/c7T9hB723
4T9yrRHJbygTvQD8BJBADgRy7+XInCp01V4nAJZSu20qopEg082SdWK9FwARAQAB
tCZLYWxpIExpbnV4IFJlcG9zaXRvcnkgPGRldmVsQGthbGkub3JnPokCVQQTAQoA
PwIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AWIQRExlE6jk+z0wh191jtRE/w
fY0L9gUCYe/xTgUJGD63pgAKCRDtRE/wfY0L9ofUD/9zichMeQ5+XxHnpHTSmUNR
9eCcis6NGIbW+hTfSxSttfCQBrxKGfYXwVcqGRIiSDp9FcfqH5UsgPOzgJzmLBLV
i0HfMRDpcCWJzk8VfWde/5Hv0P0XSx/Y+VR7PMJVOzWkF7o0kM4bITx3M5BYY08s
leoZMNZo9sSR0GdzbXoIXkuBwMG+nw0qjfsyI8Qcsi52Uk8YhdCkgaAb8vYyxMwO
qKJ6SIIENT6ycyZw4ueFZXZY/RYPJFvWZEYB0cFOMbNwlrXFUZyr4fDdPruaPlZW
zBIU8jwEE372frdRuXilJ2Q+Me9jhSxvnJegJsHDdgeLU6IDeAiaAaTzvufr3KmA
YifZ1Q20+DzdN5RZ5+3vNV9cihVb3qizSUe0y6LfpPeIPoa+ENzT4WqhP6rfMMhF
2KcwhNFP+faB+qs79YqIWnChrJNiE5HQDDgP6DY1ETmjj6Bo+DC9RyasWT5pSJYA
8rOVJ+1bE4sxlqtvDVlAdR1LwIpHeskz4o/lAMPHSNTX2WBDJdYvhT28xTC3cYlA
kcdpvBbjj7C4VqgMvsPLg13lfR/A28ADO6AxY323+OpPv6crsDbYOcIBpwBgHb96
AYyottiEfNnLBCysR/m34TdlYvFW0KDYsbMYLCJH/uzJK3l8TCdVBfkzDMMctSFV
nFY/xHhDFweArXNHru2CJLkCDQRPVNQoARAAoMOCt6yDngNUawaFLqFzzkQ2UDt1
LyWMM5qRusYmVW7DbMqRgl816AhW3qGXlpET2QDK/C7np8kiwkx22cWkK2W7e877
bKGX1jH0k8jIZWxE15pBCBkTk+zb6elC263qiw36jxAlEnwd4eP0OAY6SxD9xi5H
fJ7zXO+2hF4bVgofRGNmr5IA9SPL0yRJo+dNm3Sh+MhdNMpvJpOdk0PWqq1ZP9LC
```

Right Ctrl

1. Can someone spy on your data if your connection is not secured?
   (A) Yes (B) No

2. Why do we need HTTPS?
   (A) For privacy and identification (B) For faster websites
   (C) For privacy, integrity, and identification (D) For identification only

3. In the context of HTTPS, what does integrity mean?
   (A) That my browser has ethics
   (B) That communication is not being tampered with
   (C) That the website I am visiting is honest
   (D) That the internet is strong and durable

Reference: The differences between HTTPS, SSL, and TLS

https://howhttps.works/https-ssl-tls-differences/

1. Can someone spy on your data if your connection is not secured?

   (A) Yes (B) No

2. Why do we need HTTPS?

   (A) For privacy and identification (B) For faster websites

   (C) For privacy, integrity, and identification (D) For identification only

3. In the context of HTTPS, what does integrity mean?

   (A) That my browser has ethics

   (B) That communication is not being tampered with

   (C) That the website I am visiting is honest

   (D) That the internet is strong and durable

Reference: The differences between HTTPS, SSL, and TLS

https://howhttps.works/https-ssl-tls-differences/

1. In _____cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption).

   (A) Symmetric-key
   (B) Asymmetric-key
   (C) Public-key
   (D) None of the above

2. In _____ cryptography, everyone has access to everyone's public key.

   (A) Symmetric-key
   (B) Asymmetric-key
   (C) Both (A) and (B)
   (D) None of the above

Reference: Chapter 28 Quiz

https://highered.mheducation.com/sites/0072967722/student_view0/chapter_28_quiz.html

1. In _____cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption).

   (A) Symmetric-key
   (B) Asymmetric-key
   (C) Public-key
   (D) None of the above

2. In _____ cryptography, everyone has access to everyone's public key.

   (A) Symmetric-key
   (B) Asymmetric-key
   (C) Both (A) and (B)
   (D) None of the above

Reference: Chapter 28 Quiz

https://highered.mheducation.com/sites/0072967722/student_view0/chapter_28_quiz.html

1. What is hashing in the context of security?

Answer: A hash function is any function that can be used to map data of arbitrary size to fixed-size values. The values returned by a hash function are called hash values, hash codes, digests, or simply hashes.

2. Why are hash functions used to store passwords in DB?

Answer: Since hash is a one-way compression function, instead of storing the password itself, its hash value is stored. The user enters their password at the time of login. Then the hash value of the entered password will be compared with the stored hash value in DB and if both matched then the user will be logged in.

Reference: 20 Web Security Questions

https://circuit.bcit.ca/repository/islandora/object/repository%3A1362/datastream/PDF/view

1. A _____ serves as the trusted third-party agency that is responsible for issuing the digital certificates.

Answer: Certificate Authority (CA)

Explanation: A CA is an entity that is responsible for issuing digital certificates. These certificates are used to verify the authenticity and integrity of digital communications and transactions. The CA acts as a trusted third-party agency, ensuring that the certificates are issued to the correct entities and that they can be trusted by relying parties. The CA uses cryptographic algorithms to generate and sign these certificates, providing a secure and reliable mechanism for establishing trust in the digital world.

Reference: How Much Do You Know About Digital Certificate? Chapter 12 Quiz
https://www.proprofs.com/quiz-school/story.php?title=chap-12_4
Reference: Digital Certificates Explained - How digital certificates bind owners to their public key
https://www.youtube.com/watch?v=5rT6fZUwhG8