Gmail

Krishna chaitanya <ekrishnachaitanya2004@gmail.com>

# Assignment on Securing Data for CS50 Cybersecurity

1 message

**Google Forms** <forms-receipts-noreply@google.com>
To: ekrishnachaitanya2004@gmail.com

1 June 2024 at 17:11

Google Forms

Thanks for filling in Assignment on Securing Data for CS50 Cybersecurity

Here's what was received.

## Assignment on Securing Data for CS50 Cybersecurity

All assignments in CS50 Cybersecurity are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. **Please do not resubmit an assignment if you have already obtained a passing score**--we consider that spam, and if detected, the submission will be deleted, meaning you will not receive the score back anyway. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50cy (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

ekrishnachaitanya2004@gmail.com

Name *

KRISHNA CHAITANYA

edX Username *

eKRISHNA2004

What is your GitHub username? *

If you do not already have a GitHub account, you can sign up for one at https://github.com/join. You can then use this account to log in to cs50.me/cs50cy to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50cy is important!

- **Be certain the username you provide is correct!** If you provide the wrong username, you will not be able to see your scores.
- **Your GitHub username should not be changed while you are taking this course.** The current gradebook system is not designed to accommodate name changes.
- **Be sure to remove extraneous characters,** such as an @ prefix. Do not input a URL or email address, just your username.

ekrishnachaitanya2004

City, State, Country *

Srikalahasthi,Andhra pradesh,India.

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source, including non-course-sanctioned generative AI tools or (b) another student's work in the course, in *any* of the course's five assignments or the final project, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard. **The full essence of all work you submit to this course should be your own.**

● I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any answers in this course.

Characterize the difference between a database *hack* and a database *leak*.

A database hack is an intentional and harmful attack aimed at stealing ,changing or destroying data often using methods like sql injection malware and phishing it needs high technical skill and leads to major financial loss legal trouble and damage to reputation in contrast.A database leak is usually accidental caused by errors like misconfigured servers or unsecured backups leaks happen due to carelessness or poor security practices resulting in data exposure fines and loss of trust the main difference is that hacks are deliberate attacks while leaks are unintentional exposures

In what sense might files not actually be deleted even if you empty the recycle bin on Windows or empty the trash on macOS?

Deleting a file and emptying the trash doesn't always ensure complete removal because several factors can prevent it. When you delete a file, it typically removes its directory entry but not the actual data, which can still be recovered until overwritten. Temporary file copies, system snapshots, and cloud storage backups can all hold onto deleted files. Additionally, system restore points and third-party backup software may contain copies. Specialized file recovery tools can scan for and retrieve deleted files since the operating system doesn't immediately overwrite the data. To ensure complete deletion, consider using secure erase tools or specialized software designed for permanent file destruction.

How do quantum computers differ from traditional (non-quantum) computers?

Regular computers operate like standard switches, functioning in binary as either on (1) or off (0). In contrast, quantum computers resemble dimmer switches, capable of existing in states between on and off, allowing them to explore numerous possibilities concurrently, rendering them exceptionally potent for specific tasks.

What is the term for the prevailing method via which public-key (i.e., asymmetric) cryptography enables two parties to establish a *shared secret*, even over an insecure (i.e., unencrypted) channel?

key exchange

What is a salt, in the context of this lecture?

Salt, in the context of password hashing, is a random value added to a password before it's hashed. It prevents attackers from easily cracking passwords even if they steal the hashed password file. Adding salt makes it much less likely that two users with the same password will have the same hashed password.

Suppose that Alice and Bob need to coordinate a meeting, as by exchanging emails using Microsoft Outlook, a popular client for email.

If their emails are encrypted in-transit, who (besides Alice and Bob, or anyone with access to their computer) might nonetheless be able to read the emails if anyone, and why?

An important security measure doesn't ensure full email privacy for Alice and Bob, even though their emails are encrypted while moving between servers, there's a chance that email server providers can access the content. This happens because the emails have to be processed on these servers for tasks like spam filtering or malware scanning, and the servers possess the decryption keys needed to unlock the emails during this process. However, it's crucial to note that server providers usually adhere to regulations and privacy standards, so they probably wouldn't read emails for routine purposes.

Suppose that you have been hired to perform some work for Charlie. After agreeing to terms, you send the contract to Charlie via email, and, later that day, you receive a digitally signed copy from an email address that *appears* to belong to Charlie but isn't the one to which you sent the contract originally.

How can you be as certain as possible, **technologically** (that is, without consulting Charlie) that Charlie was the one who digitally signed the contract?

Though the email seems from Charlie, tech can help raise suspicion but not guarantee his identity for the signed contract. Check the signature properties in your email client. Look for a reputable Certificate Authority issuing the signature and use their online tools to verify it. If the certificate includes an email address, compare it to where you sent the contract. A different address suggests spoofing. Analyze the email header for inconsistencies in the sender's domain name. While these steps build confidence, they can't be foolproof. For certainty, contact Charlie directly through a trusted channel to confirm the signed document.

MD5 is an example of a still popular hashing algorithm that has been in use since the early 1990s. Read this article about MD5 before continuing on.

Note that MD5 is a 128-bit algorithm, meaning its digests (i.e. hash values) are always 128 bits in length, and therefore there are 2^128 unique digests available. Thus, understand that the article's critique that there is a "high potential for collisions," while not invalid or indeed even incorrect, is perhaps something that should be understood with a bit of context.

Suppose that a company has made a large file available for download via its website. Why might they also make available the MD5 hash of that file (as is indeed a common practice)?

Providing the MD5 hash of a file alongside its download offers multiple benefits. Firstly, users can verify the integrity of the downloaded file by comparing its MD5 hash to the provided one, ensuring it hasn't been tampered with during download. Additionally, users can use the MD5 hash as a checksum to confirm the data received matches the original file, detecting even minor changes indicative of corruption. This practice fosters trust and confidence by demonstrating transparency in file delivery and security measures. Moreover, in the event of transmission or storage errors, users can swiftly identify discrepancies between the downloaded file and its expected MD5 hash, prompting necessary actions. Lastly, in restricted or unreliable internet environments, users can utilize the MD5 hash to verify file integrity after downloading through alternate means, ultimately enhancing data integrity, user trust, and ensuring a dependable download experience.

Identify one or more significant differences between a cipher and a hash.

A cipher is like a secret code that scrambles and unscrambles messages, used to keep data private during transmission or storage. Think of it as locking and unlocking a box with a key. A hash function, however, is more like a digital fingerprint. It takes any input, like a file or a password, and creates a unique string of characters that represent it. This fingerprint is used to ensure that data hasn't been tampered with and to verify passwords without storing them directly.

Otkz ***D zvmizy v amzz kjdio!*** di ocz wjs wzgjr.

No, the above isn't random typing! :)

I earned a free point!

## Feedback

How did you find the difficulty of this assignment?
*

| | 1 | 2 | 3 | 4 | 5 | |
|---|---|---|---|---|---|---|
| Too easy | ○ | ○ | ● | ○ | ○ | Too hard |

About how many MINUTES would you say you spent on this assignment?
*

Just to set expectations for future students.

300