✓ Characterize the difference between a database *hack* and a database *leak*. 1/1

Hacking a database means that a person or organization uses it for their own purposes and obtaining information, but a database leak means that there is a hole or flaw in the system that causes information to be leaked. :)

✓ In what sense might files not actually be deleted even if you empty the recycle bin on Windows or empty the trash on macOS? 1/1

When the user deletes a file or data from these systems, it is not completely deleted, even if it is moved to the recycle bin and deleted from there, it is still not completely deleted and is in a different location of the hard save. and it can be overwritten again. Safe removal should be used to remove them completely

✗ How do quantum computers differ from traditional (non-quantum) computers? 0/1

1. Normal computers have gone through a long process of bug and upgrade and error correction during this time, but quantum computers are still new, still far from being perfect and have not yet gone through the debugging process.
2. Normal computers use binary bits, and quantum computers use qubits, which are very powerful.
3. Quantum computers need a very low temperature compared to normal computers.

✓ 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? 1/1

DIFFIE-HELLMAN key exchange

✓ What is a salt, in the context of this lecture? 1/1

In hashing, we discussed that we may have two same passwords, the same output may occur in the hashing process.
To prevent this, we give two inputs, one salt, for example 20, and then we give the password, the output of which starts with 20, and the continuation of the hash is completely different.
In this way, we avoid repeating two similar passwords.

✓ Suppose that Alice and Bob need to coordinate a meeting, as by exchanging emails using Microsoft Outlook, a popular client for email. 1/1

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?

We have 3 different factions that can access information.
One is those who provide the platform, such as Google Outlook, the second is the sender of the information, and the third is the receiver of the information. It's the same here, except for Bob and Alice, there's also the Google Outlook platform that accesses the information.

✗ 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. 0/1

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

By right clicking and checking the details of the message, we will come to the conclusion that it is really from Charlie or not.
But it is possible that his email was hacked.

✗ 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. 0/1

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)?

It is true that it may be vulnerable, but it is still used for several reasons
We give it any input value, whether it is short, long, or 1 digit, it outputs a 128-bit hash and has a high speed.

✓ Identify one or more significant differences between a cipher and a hash. 1/1

CIPHER: If we give it 10 input characters, it outputs 10 characters, that is, it replaces every character, and except for this mode, they are reversible, or it can be said that they have a photo function.
HASH: They are not reversible, they are a one-way function, and no matter how long or medium the input is, or even 1 character, it returns a fixed-length output.

✓ Otkz ***D zvmizy v amzz kjdio!*** di ocz wjs wzgjr. 1/1

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

i earned a free point! ✗

Feedback