Computer Science Principles
Lesson: April 9, 2020

Learning Target:

In this lesson, the goal is to build student understanding of the Internet as a set of computers exchanging bits in the form of packets, and for students to identify the components of their digital footprint.

A Question to Ponder:

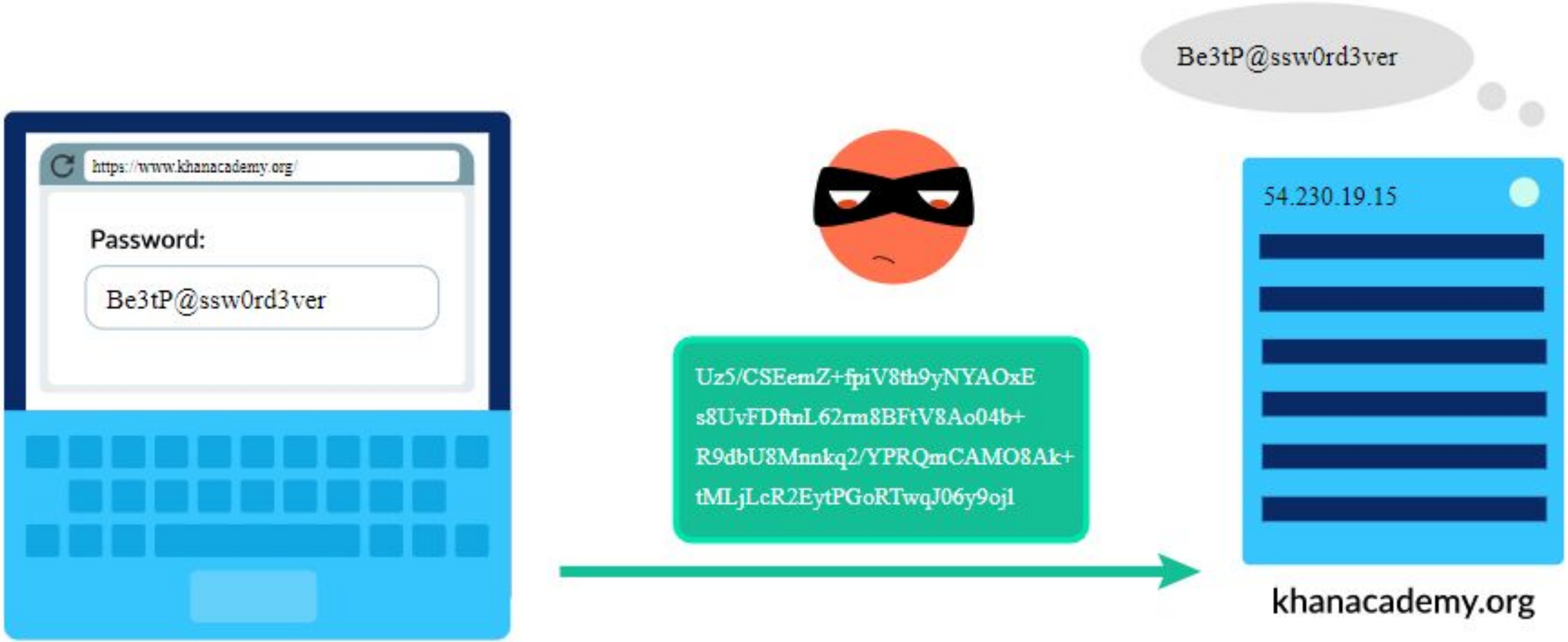
Think about the last time you were in the same room with a friend and you were both on the internet, looking up information and sending emails. What prevented your internet requests from getting mixed up with your friend's requests? Write your answers in your journal or discuss it with a friend or a family member...

Practice:
How can computers send private data?

We send a whole lot of secure information around the Internet: emails with details on our private life, passwords that we type into login screens, tax documents that we upload to servers.The TCP/IP protocols send that private data in packets on the same routes as everyone else's data, and

https://www.khanacademy.org/
Password:
****
Be3tP@ssw0rd3ver
54.230.19.15
khanacademy.org

That's where encryption comes in: encrypting data means that we scramble the original data to hide the meaning of the text, while still making it possible for the data to be unscrambled using a secret key.Encryption enables two people (or computers!) to share private information over


https://www.khanacademy.org/
Password:
Be3tP@ssw0rd3ver
Uz5/CSEemZ+fpiV8th9yNYAOxE
s8UvFDftnL62rm8BFtV8Ao04b+
R9dbU8Mnnkq2/YPRQmCAMO8Ak+
tMLjLcR2EytPGoRTwqJ06y9oj1
Be3tP@ssw0rd3ver
54.230.19.15
khanacademy.org

How can computers send private data?

- In this video , security researcher Mia Epner explains the basics of encryption algorithms.
- After that, we'll dive deeper into the encryption algorithms, starting with the simplest symmetric encryption technique and moving on to the asymmetric technique of public key encryption.
- Finally, we'll learn how the TLS protocol adds a layer of encryption on top of TCP/IP, using both symmetric and public key encryption to send private data around the Internet.

By clicking the links below, you can read about and practice different types of ciphers and encryption techniques...Be certain to take notes and practice these encryptions in your notebook.

Encryption, decryption, and cracking

Symmetric encryption techniques

More Practice: Symmetric Encryption

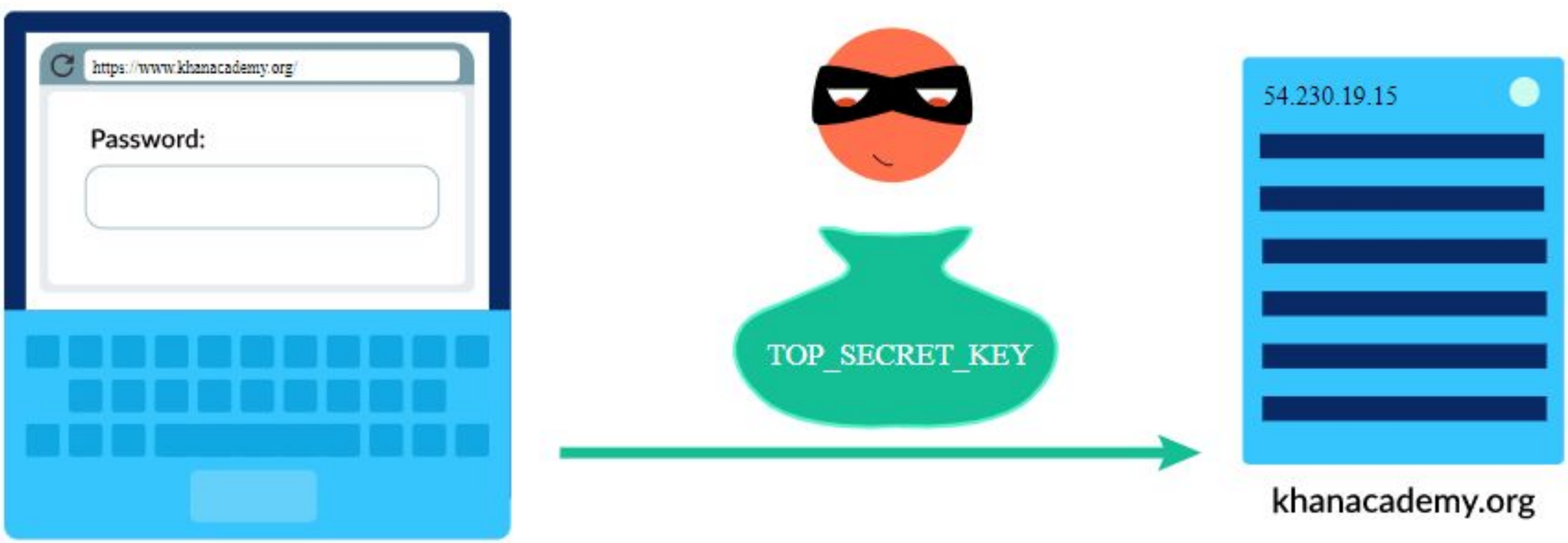
Public key encryption

On the Internet, two computers often want to exchange secure data with each other. When I type my password into the login screen, I want my computer to send that data safely to the data servers. I do *not* want to worry that a cybercriminal might be monitoring my Internet traffic and watching the password go across the wires.

https://www.khanacademy.org/
Password:
****
Be3tP@ssw0rd3ver
54.230.19.15
khanacademy.org

Public key encryption

Symmetric encryption techniques rely on both the sender and receiver using the *same key* to encrypt and decrypt the data. How can my computer and the server exchange the key securely? If a cybercriminal can see my password go across the wires, then they can also see an encryption



Public key encryption

Public key encryption to the rescue! It's an asymmetric encryption technique which uses *different keys* for encryption and decryption, allowing computers over the Internet to securely communicate with each other.

Let's step through the high-level process of public key encryption. Click here to learn more!

For added Practice, click here!

Transport Layer Security (TLS)

Computers send packets of data around the Internet using the TCP/IP protocols. These packets are like letters in an envelope: an onlooker can easily read the data inside them. If that data is public information like a news article, that's not a big deal. But if that data is a password, credit card number, or confidential email, then it's risky to let just anyone see that data.The **Transport Layer Security (TLS)** protocol adds a layer of security on top of the TCP/IP transport protocols. It takes advantage of both symmetric encryption and public key encryption for securely sending private data, and adds additional security features like authentication and message tampering detection.

Click here to Step Through the entire Process from start to Finish

Click here for added practice on Transport Layer Secuity

- **Tomorrow: HTTP and HTML: Global Document and data Sharing. What is the World Wide Web?**